A New Use of Friedman's Translation: Interactive Realizability

Federico Aschieri, Stefano Berardi

Dipartimento di Informatica
Università di Torino
Italy

Abstract

Friedman's translation is a well-known transformation of formulas. The Friedman translation has two properties: i) it validates intuitionistic theorems – if a formula is intuitionistically provable, then so it is its Friedman translation; ii) it is suitable for program extraction from classical proofs – the intuitionistic provability of the Friedman translation of the negative translation of a for-all-exist-formula implies the intuitionistic provability of the formula itself. However, the Friedman translation does not validate classical principles, like the Excluded Middle.

Here, we define a restricted Friedman translation which both validates the Excluded Middle and Skolem axiom schemata restricted to Σ_1^0-formulas and it is also suitable for program extraction from classical proofs using such principles: the intuitionistic provability of the restricted Friedman translation of a for-all-exist-formula implies the intuitionistic provability of the formula itself. Then we introduce a learning-based Realizability Semantics for Heyting Arithmetic with all finite types, extended with the two previous axiom schemata. We call this semantics "Interactive Realizability", and we characterize it as the composition of our restricted Friedman translation with Kreisel modified realizability. As a corollary, we show that Interactive Realizability is, in a sense, "axiom-driven", while the other Realizability Semantics for Classical Arithmetic, like the semantics of Krivine, are "goal-driven".

Keywords: learning-based realizability, Friedman's translation, classical Arithmetic
2010 MSC: 03F03, 03F30, 03F55

1. Introduction

In the past years, many computational interpretations of Classical Arithmetic have been put forward. Under a first classification, they fall into two large categories: *direct* and *indirect* interpretations. Among the indirect interpretations one finds the negative translations followed either by Dialectica interpretations [13], [30] (see e.g. Kohlenbach [19]) or by intuitionistic realizability interpretations combined with Friedman's translation [12] (see e.g. Berger and Schwichtenberg [10]). Among the direct interpretations, there are different versions of Classical Realizability (Krivine's [22] and Avigad's [6]), there is Coquand game semantics [11], cut-elimination and normalization of classical proofs [14] (under Curry-Howard correspondence of not), and the epsilon substitution method [23] (the Kreisel no-counterexample interpretation [20] is an easy corollary of the other ones). More recently, another Classical Realizability interpretation for Heyting Arithmetic with Excluded Middle and Skolem axioms over Σ^0_1-formulas has been introduced by Aschieri, Berardi and de' Liguoro [8], [1], [9]: it is based on the notion of learning and it is called the "Interactive Realizability". The goal of this paper is to compare Interactive Realizability with the other notions of Classical Realizability, using Friedman's translation and Kreisel modified Realizability as tools.

On a first sight, these computational interpretations of Classical Arithmetic may appear completely different. However, this is not the case and it is often possible to find unifying concepts. A common way of studying and relating the various computational interpretations of Classical Arithmetic is, first, to characterize them in terms of translations of Classical into Intuitionistic Arithmetic and secondly, to compare the resulting translations. In the case of Classical Realizability interpretations one usually has

Classical Realizability

$$=$$

Negative Translation + Friedman's Translation + Modified Realizability

For example, Avigad [7] characterized its own Classical Realizability in terms of a special negative translation followed by Friedman's translation again followed by Kreisel's modified realizability [21]; similarly did Towsner [32]. Oliva and Streicher [27] managed to do the same for Krivine's classical realizability for Classical Analysis. Miquel [25] used their characterization to compare the algorithms extracted from proofs of Σ^0_1-formulas – either obtained by using Krivine's realizability or Oliva and Streicher's characterization – and to conclude they are basically the same. All these results characterize classical realizability in the following way: a *classical realizer* of a formula B is an *intuitionistic realizer of some Friedman translation of some negative translation of* B.

In this paper we build over this research line and we investigate the relationship between Interactive Realizability and Friedman's translation. We shall prove (from an idea of the first author) that Interactive Realizability for Heyting Arithmetic in all finite types HA^ω, with Excluded Middle EM_1 and Skolem axioms SK_1 over Σ^0_1-formulas, can be understood as a new way of using Friedman's translation, a way that avoids the use of negative translations for program extraction purposes. Interactive Realizability restricts the family of goal-formulas in Friedman's translation, in order to interpret each instance of Excluded Middle used in the proof by some constructive principle. While in the usual Friedman's A-translation the goal-formula A is some Σ^0_1-property that one wants to prove (it is "goal-driven"), in ours the goal is fixed once and for all, does not depend on the particular proof one is considering and consists in learning something about the Skolem functions interpreting the Excluded Middle. More precisely, we will show that learning-based realizability can be decomposed in a fixed Friedman $\mathscr{A}$-translation followed by Kreisel's modified realizability, as follows:

Interactive Realizability

$$=$$

Friedman's $\mathscr{A}$-Translation + Modified Realizability

The fixed formula $\mathscr{A}$ has a free variable $s : \mathtt{N}^2 \to \mathtt{N}$ and says: "there exists a counterexample to the fact that s is a Skolem function solving the Halting problem". More precisely, $\mathscr{A}$ asserts that s is *not* a Skolem function for the formula $\forall x^{\mathtt{N}} \forall y^{\mathtt{N}} \exists z^{\mathtt{N}} \mathscr{T}xyz$, where $\mathscr{T}$ is Kleene's predicate. In other words, $\mathscr{A}$ says that the familiar full type structure built over natural numbers is not a Tarski model of $\mathsf{HA}^{\omega} + \mathsf{EM}_1 + \mathsf{SK}_1$, whenever the function s is interpreted as a Skolem function solving the Halting problem, and that there is a counterexample supporting this assertion. We observe that a counterexample to the assertion that s is a Skolem function solving the Halting problem is just a triple of numbers (n, m, l) such that $\mathscr{T}nml = \mathtt{True}$ and $\mathscr{T}nms(n, m) = \mathtt{False}$. This is true because if s is not such a Skolem function, it makes false the Skolem axiom:

$$\forall x^{\mathtt{N}} \forall y^{\mathtt{N}} \forall z^{\mathtt{N}}.\ \mathscr{T}xyz \to \mathscr{T}xys(x, y)$$

We shall use this characterization to stress the similarities, but also the differences, between Interactive Realizability and the other Classical Realizability semantics proposed so far. Namely, all these Realizability semantics are related to some Friedman's translation, but in Interactive Realizability the negative translation is eliminated, and the restricted Friedman translation implicit in Interactive Realizability validates the Excluded Middle and Skolem axioms (it is "axiom-driven"). In particular, an *interactive realizer* of a formula B is characterized just as an *intuitionistic realizer of the Friedman $\mathscr{A}$-translation of B*. The result seems to accord with the intuition that learning-based realizability describes "locally" the constructive ideas hidden in classical proofs, thanks to the interpretation of classical principles with Skolem functions and learning algorithms.

1.1. Plan of the Paper

In section §2 we prove that there exists a restricted Friedman's translation validating Excluded Middle and Skolem axiom schemata (both restricted to Σ^0_1-formulas), which at the same time still allows program extraction from profs of Π^0_2-formulas. In the rest of the paper we define the Interactive Realizability Semantics, corresponding to such restricted Friedman's translation.

In section §3 we introduce a term calculus in which Interactive, learning-based realizers are written, namely an extension of Gödel's system T plus a constant symbol for a Skolem function Φ.

In section §4, we extend Interactive Realizability, as described in [1], to $\mathsf{HA}^{\omega} + \mathsf{EM}_1 + \mathsf{SK}_1$, an arithmetical system with functional variables.

In section §5, we compare Interactive Realizability with Kreisel's no-counterexample interpretation and we give an example of interactive realizer.

In section §6 we conclude our characterization of Interactive Realizability in terms of Kreisel's modified Realizability + restricted Friedman's translation.

2. A restricted version of Friedman's Translation

In this section we first remark how Friedman's translation does not validate Excluded Middle for Σ^0_1-formulas, and then how a restricted version of it does. In the rest of the paper we define the Interactive Realizability Semantics, which may be defined as the composition of Kreisel's modified Realizability with our restricted Friedman's translation.

2.1. The Friedman Translation

The Friedman translation is a strikingly simple device introduced by Friedman [12] in order to prove closure of intuitionistic systems S under Markov's rule:

$$S \vdash \neg\forall x^{\mathtt{N}} \neg P(x) \implies S \vdash \exists x^{\mathtt{N}} P(x)$$

where P is any decidable quantifier free formula, possibly with some other free variables besides x.

The translation gives a reasonable semantics to formulas that are derived in a possibly inconsistent universe, in which some arbitrary universal statement is assumed to be true. In such a world, false statements can be proved by perfectly valid arguments, since the assumption of the world may be false. For example, one may prove

$$\mathsf{HA} + \forall x^{\mathtt{N}} \neg P(x) \vdash \bot$$

as lemma in a classical proof of $\exists x^{\mathtt{N}} P(x)$. Tarskian semantics is therefore no longer adequate. The idea of Friedman's translation is to change the meaning of formulas in such a way that even false formulas are interpreted by true ones, carrying interesting constructive information. In a universe in which a false assumption is made, the only way of recovering from the disaster of some derived false atomic formula Q is pointing out the concrete false consequence of the false assumption that is to blame for deriving Q. If the false assumption is $\forall x^{\mathtt{N}} \neg P(x)$, the new meaning of Q is

$$Q \vee \exists x^{\mathtt{N}} P(x)$$

In words, if Q is derived from the assumption $\forall x^{\mathtt{N}} \neg P(x)$, either Q is true, or Q is false and thus some false consequence $\neg P(n)$ of $\forall x^{\mathtt{N}} \neg P(x)$ must have been used in the derivation of Q. Thus $P(n)$ must be true and $\exists x^{\mathtt{N}} P(x)$ must hold.

The following theorem, from [12], is well known and holds for many systems. Here, we shall focus on the system HA^ω (see section §4.1 for details):

Theorem 1 (Friedman's A-Translation). *Given any formulas A, B, where A has not free variables occurring bound in B, let us denote with B^A the formula resulting from B by replacing every atomic formula Q of B with $Q \vee A$. If Γ is a set of formulas and*

$$\mathsf{HA}^\omega + \Gamma \vdash B \textit{ and } \mathsf{HA}^\omega \vdash F^A \textit{ for every } F \in \Gamma$$

then

$$\mathsf{HA}^\omega \vdash B^A$$

The theorem is proved by straightforward induction on proof length (see Friedman [12]), and crucially depends on the fact that the A-translation of every axiom of HA^ω is provable in HA^ω.

Now suppose that

$$\mathsf{HA}^\omega \vdash \neg\forall x^{\mathtt{N}} \neg Q(x)$$

where Q is any quantifier-free formula. Then, by theorem 1

$$\mathsf{HA}^\omega \vdash (\neg\forall x^{\mathtt{N}} \neg Q(x))^{\exists x^{\mathtt{N}} Q(x)}$$

But this latter formula implies $\exists x^{\mathtt{N}} Q(x)$ in HA (see Friedman [12]) and thus

$$\mathsf{HA}^{\omega} \vdash \exists x^{\mathtt{N}} Q(x)$$

Therefore HA^{ω} is closed under Markov's rule.

This closure property of HA^{ω} is exploited for program extraction purposes, in connection with Gödel's double negation translation (again, see [12]). In particular, if PA^{ω} is the classical version of HA^{ω}, one can show that

$$\mathsf{PA}^{\omega} \vdash \forall x^{\mathtt{N}} \exists y^{\mathtt{N}} P(x,y) \implies \mathsf{HA}^{\omega} \vdash \forall x^{\mathtt{N}} \neg \forall y^{\mathtt{N}} \neg P(x,y)$$

and thus by closure of HA^{ω} under Markov's rule

$$\mathsf{PA}^{\omega} \vdash \forall x^{\mathtt{N}} \exists y^{\mathtt{N}} P(x,y) \implies \mathsf{HA}^{\omega} \vdash \forall x^{\mathtt{N}} \exists y^{\mathtt{N}} P(x,y)$$

We notice that the preliminary use of the negative translation *before* Friedman's translation is necessary to obtain the above result, since the following generalization of theorem 1 is false:

$$\mathsf{PA}^{\omega} \vdash B \implies \mathsf{HA}^{\omega} \vdash B^{A}$$

This is due to the fact that HA^{ω} does not prove the A-translation of the Excluded Middle for *every* formula A, because if A is refutable then $B^A \Leftrightarrow B$. A-translation proves only the A-translation of the double negation translation of Excluded Middle. Therefore, A-translation alone cannot eliminate classical reasoning. It is thus intriguing to ask whether Friedman's translation *alone* is enough for program extraction from proofs of Π^0_2-formulas in the system $\mathsf{HA}^{\omega} + \mathsf{EM}_1 + \mathsf{SK}_1$. More precisely: is there a formula $\mathscr{A}$ such that

$$\mathsf{HA}^{\omega} \vdash \mathsf{EM}_1^{\mathscr{A}} \qquad \mathsf{HA}^{\omega} \vdash \mathsf{SK}_1^{\mathscr{A}}$$

and *for all* atomic formulas $P(x,y)$ we have the following correctness property:

$$\mathsf{HA}^{\omega} \vdash (\forall x^{\mathtt{N}} \exists y^{\mathtt{N}} P(x,y))^{\mathscr{A}} \implies \mathsf{HA}^{\omega} \vdash \forall x^{\mathtt{N}} \exists y^{\mathtt{N}} P(x,y) \quad ?$$

If there is such a formula, then by theorem 1 one has:

$$\mathsf{HA}^{\omega} + \mathsf{EM}_1 + \mathsf{SK}_1 \vdash \forall x^{\mathtt{N}} \exists y^{\mathtt{N}} P(x,y) \implies \mathsf{HA}^{\omega} \vdash \forall x^{\mathtt{N}} \exists y^{\mathtt{N}} P(x,y)$$

allowing program extraction from classical proofs in the system $\mathsf{HA}^{\omega} + \mathsf{EM}_1 + \mathsf{SK}_1$ just by using Kreisel's modified realizability for HA^{ω}. The answer, as we shall see, is positive: Interactive Realizability defines in a natural way a formula $\mathscr{A}$ with the desired properties. We observe that this formula *does not* vary with the particular Π^0_2-formula one wants to prove, whereas in the standard use of Friedman's translation the goal formula always does. For the sake of simplicity, in this section we assume

$$\mathsf{EM}_1 := \forall x^{\mathtt{N}} \forall y^{\mathtt{N}}.\ \exists z^{\mathtt{N}}\ \mathscr{T}(x,y,z) \vee \forall z^{\mathtt{N}} \neg_{\mathtt{Bool}} \mathscr{T}(x,y,z)$$

since all other instances of the Excluded Middle on Σ^0_1-formulas can be derived from the instance over Kleene's predicate (see definition 3 of section §3). Similarly, we also assume

$$\mathsf{SK}_1 := \forall x^{\mathtt{N}} \forall y^{\mathtt{N}} \forall z^{\mathtt{N}}.\ \mathscr{T} xyz \Rightarrow_{\mathtt{Bool}} \mathscr{T} xy\Phi(x,y)$$

2.2. A New Way of using Friedman's Translation

To the same extent that Friedman's translation deals with provability under possibly false assumptions, Interactive, learning-based realizability (see section §4) deals with computations under possibly false computational hypotheses. The first repairs false proved statements by pointing out the actual concrete assumption that causes the inconsistency; the second repairs wrong computational results by spotting some wrong value of the Skolem function that produced some mistake. In particular, the very idea behind learning-based realizability is to make assumptions about the values of the Skolem function Φ for the predicate $\mathscr{T}$ and, thanks to them, carry out computations even in situations in which one cannot effectively compute the *right* values of Φ. By a continuity argument, given any approximation $s : \mathtt{N}^2 \to \mathtt{N}$ of Φ, one knows that if s satisfy the following axiom

$$\mathsf{SK}_1[s] = \forall x^{\mathtt{N}} \forall y^{\mathtt{N}} \forall z^{\mathtt{N}}.\ \mathscr{T}xyz \Rightarrow_{\mathtt{Bool}} \mathscr{T}xys(x,y)$$

for a sufficient number of particular choices for x, y, z, then a realizer of a Σ^0_1-formula will be able to compute a right witness when using s in place of Φ. If, instead, the witness computed is incorrect, then one knows that $\mathsf{SK}_1[s]$ is false, and the task of the realizer is to spot a wrong value of s and to correct it with a right one. The realizer effectively finds out numerals n, m, l such that

$$\mathscr{T}nml \wedge \neg_{\mathtt{Bool}} \mathscr{T}nms(n,m)$$

and thus recognizes that

$$\mathscr{A}(s) := \exists x^{\mathtt{N}} \exists y^{\mathtt{N}} \exists z^{\mathtt{N}}.\ \mathscr{T}xyz \wedge \neg_{\mathtt{Bool}} \mathscr{T}xys(x,y)$$

holds, which is classically equivalent to the negation of $\mathsf{SK}_1[s]$. $\mathscr{A}(s)$ asserts that there exists a *counterexample* to the fact that s is a Skolem function for $\mathscr{T}$. In general, the behavior of a learning-based realizer of an atomic formula Q, is to realize, in Kreisel's sense, the formula

$$Q \vee \mathscr{A}(s)$$

(but possibly providing multiple witnesses of $\mathscr{A}(s)$). We choose $\mathscr{A}(s)$ as the formula of the Friedman translation we were seeking, where s is a free variable denoting any map of type $\mathtt{N}^2 \to \mathtt{N}$.

We now prove that $\mathscr{A}(s)$ is exactly the formula for the Friedman translation we asked for.

Theorem 2 (A New Use of Friedman's Translation). *Let $s : \mathtt{N}^2 \to \mathtt{N}$ be a variable and let*

$$\mathscr{A}(s) := \exists x^{\mathtt{N}} \exists y^{\mathtt{N}} \exists z^{\mathtt{N}}.\ \mathscr{T}xyz \wedge \neg_{\mathtt{Bool}} \mathscr{T}xys(x,y)$$

Then we have

1. $\mathsf{HA}^\omega \vdash (\mathsf{SK}_1[s])^{\mathscr{A}(s)}$
2. $\mathsf{HA}^\omega \vdash (\mathsf{EM}_1)^{\mathscr{A}(s)}$

PROOF. 1. Since

$$(\mathsf{SK}_1[s])^{\mathscr{A}(s)} = \forall x^{\mathtt{N}} \forall y^{\mathtt{N}} \forall z^{\mathtt{N}}. \big(\mathscr{T} xyz \Rightarrow_{\mathtt{Bool}} \mathscr{T} xys(x,y) \vee \exists x^{\mathtt{N}} \exists y^{\mathtt{N}} \exists z^{\mathtt{N}}.\ \mathscr{T} xyz \wedge \neg \mathscr{T} xys(x,y)\big)$$

it is immediate to show that

$$\mathsf{HA}^{\omega} \vdash (\mathsf{SK}_1[s])^{\mathscr{A}(s)}$$

2. By definition

$$\mathsf{EM}_1^{\mathscr{A}(s)} := \forall x^{\mathtt{N}} \forall y^{\mathtt{N}}.\ \big(\exists z^{\mathtt{N}}.\ \mathscr{T}(x,y,z) \vee \mathscr{A}(s)\big) \vee \forall z^{\mathtt{N}}. \neg_{\mathtt{Bool}} \mathscr{T}(x,y,z) \vee \mathscr{A}(s)$$

We reason by cases according as to whether $\mathscr{T} xys(x,y)$ is true or not:

(a) $\mathscr{T} xys(x,y)$ is true. Then also $\exists z^{\mathtt{N}}.\ \mathscr{T}(x,y,z)$ is true and so $\mathsf{EM}_1^{\mathscr{A}(s)}$.

(b) $\mathscr{T} xys(x,y)$ is false. Then $\neg_{\mathtt{Bool}} \mathscr{T} xys(x,y)$ is true. Let us consider an arbitrary z: we want to show that $\neg_{\mathtt{Bool}} \mathscr{T}(x,y,z) \vee \mathscr{A}(s)$ holds. If $\mathscr{T} xyz$ holds, then $\mathscr{A}(s)$ is true and we have finished; if $\neg_{\mathtt{Bool}} \mathscr{T}(x,y,z)$ holds, we are done again.

We have thus concluded that

$$\mathsf{HA}^{\omega} \vdash (\mathsf{EM}_1)^{\mathscr{A}(s)} \tag{1}$$

In the rest of the paper we will define Interactive Realizability, with hindsight a semantics corresponding to the Friedman's translation we just outlined. Using Interactive Realizability, at the end of this paper we will prove that the restricted Friedman's translation of any Π_2^0-formula is correct, that is, that for any atomic formula $P(x,y)$ we have:

Theorem 3 (Correctness of the Restricted Friedman Translation).

$$\mathsf{HA}^{\omega} \vdash (\forall x^{\mathtt{N}} \exists y^{\mathtt{N}} P(x,y))^{\mathscr{A}(s)} \implies \mathsf{HA}^{\omega} \vdash \forall x^{\mathtt{N}} \exists y^{\mathtt{N}} P(x,y)$$

It is very easy to see that, classically, if the formula

$$(\forall x^{\mathtt{N}} \exists y^{\mathtt{N}} P(x,y))^{\mathscr{A}(s)}$$

is true for every s, then also the formula

$$\forall x^{\mathtt{N}} \exists y^{\mathtt{N}} P(x,y)$$

is true. Indeed, from the Axiom of Choice, one obtains the existence of a Skolem function Φ solving the the Halting problem. Thus, $\mathscr{A}(\Phi)$ must be false, since by construction there cannot be any counterexample to the fact that Φ is a Skolem function for the Halting problem (if we trust classical logic!). Thus $P(x,y)$ is equivalent to $P(x,y) \vee \mathscr{A}(\Phi)$ and thus

$$(\forall x^{\mathtt{N}} \exists y^{\mathtt{N}} P(x,y))^{\mathscr{A}(\Phi)} \rightarrow \forall x^{\mathtt{N}} \exists y^{\mathtt{N}} P(x,y)$$

is true.

However, it requires more work to prove theorem 3. A synopsis of what one has to show is the following. From a proof in HA^{ω} of the formula $\forall x^{\mathtt{N}} \exists y^{\mathtt{N}} P(x,y)^{\mathscr{A}(s)}$ one can extract an *interactive realizer* t of the formula $\forall x^{\mathtt{N}} \exists y^{\mathtt{N}} P(x,y)$. If one fixes $x = n$, from that realizer t, one directly obtains an *update procedure* (in the language of [3, 6]), which is a functional

$$\mathcal{U} : (\mathtt{N}^2 \to \mathtt{N}) \to (\mathtt{N}^3) \cup \emptyset$$

that given any function $s : \mathtt{N}^2 \to \mathtt{N}$ as argument, either returns the empty set or a triple (i, j, l) consisting in a new correct value l of the aforementioned Skolem function Φ on argument (i, j). The idea is that with an update procedure, one can construct a good enough finite approximation of Φ, which turns out to be a function f such that $\mathcal{U}(f) = \emptyset$. But the existence of such a function f can be proven in HA^ω for any update procedure representable in Gödel's system T. But then, using f, the interactive realizer t can compute a witness for the formula $\exists y^{\mathtt{N}} P(n,y)$.

The first step of our program is to introduce a term calculus $\mathcal{T}_{\text{Class}}$ in which the realizers of Interactive Realizability live.

3. The Term Calculus $\mathcal{T}_{\text{Class}}$

The content of this section is based on Aschieri and Berardi [1], with a few simplifications, namely in the notion of state. We shall review the typed lambda calculi $\mathcal{T}$ and $\mathcal{T}_{\text{Class}}$ in which learning-based realizers are written in [1]. $\mathcal{T}$ is a completely standard extension of Gödel's system T (see Girard [16]) with some syntactic sugar. The basic objects of $\mathcal{T}$ are numerals, booleans, and its basic computational constructs are primitive recursion at all types, if-then-else, pairs, as in Gödel's T. $\mathcal{T}$ also includes as basic objects finite partial functions over $\mathbb{N}$ and simple primitive recursive operations over them. $\mathcal{T}_{\text{Class}}$ is obtained from $\mathcal{T}$ by adding on top of it a Skolem function symbol $\Phi : \mathtt{N} \to \mathtt{N} \to \mathtt{N}$, denoting some map Turing-equivalent to the oracle for the Halting problem. The symbol is totally inert from the computational point of view and realizers are always computed with respect to some approximation of the Skolem map represented by Φ.

3.1. Updates

In order to define $\mathcal{T}$, we start by introducing the concept of "update", which is nothing but a finite partial function over $\mathbb{N}$. Realizers of atomic formulas will return these finite partial functions, or "updates", representing new pieces of information that they have learned about the Skolem function Φ. Skolem functions, in turn, are used as "oracles" during computations in the system $\mathcal{T}_{\text{Class}}$. Updates are new associations input-output that are intended to correct, and in this sense, to *update*, wrong oracle values used in a computation.

Definition 1 (Updates and Consistent Union). *We define:*

1. *A binary* predicate *of* T *is any closed term* $P : \mathtt{N}^2 \to \mathtt{Bool}$ *of Gödel's* T.

2. *We assume* $\mathsf{P}_0, \mathsf{P}_1, \mathsf{P}_2, \ldots$ *is any sufficiently expressive recursive enumeration of binary predicates of* T. *That is, we assume that for each numeral* n, $\mathscr{T} n = \mathsf{P}_m$ *for some* m.

3. *An update set U, shortly an* update*, is a finite set of triples of natural numbers representing a finite partial function from $\mathbb{N}^2$ to $\mathbb{N}$. We say that U is* sound *if for every $(i, n, m) \in U$, we have $\mathsf{P}_i nm = \mathtt{True}$.*

4. *Two triples (a, n, m) and (a', n', m') of numbers are* consistent *if $a = a'$ and $n = n'$ implies $m = m'$.*

5. *Two updates U_1, U_2 are consistent if $U_1 \cup U_2$ is an update.*

6. *$\mathbb{U}$ is the set of all updates.*

7. *The* consistent union *$U_1 \mathcal{U} U_2$ of $U_1, U_2 \in \mathbb{U}$ is $U_1 \cup U_2$ minus all triples of U_2 which are inconsistent with some triple of U_1.*

We think of a triple (a, n, m) belonging to a sound update as the code of a witness for $\exists y^{\mathtt{N}}.\mathsf{P}_a(n, y)$. The fact that every update is a partial *function* allows in each update at most one witness for each formula $\exists y^{\mathtt{N}}.\mathsf{P}_a(n, y)$. We remark that the enumeration $\mathsf{P}_0, \mathsf{P}_1, \dots$ can be arbitrary, as long as it is recursive, and will not play any significant role throughout the paper: it is just a simple way to give "names" to the predicates of T and to store witnesses. Only in section 6, for technical simplicity and theoretical purposes, we shall assume a particular enumeration. For implementation purposes, we may assume the enumeration $\mathsf{P}_0, \mathsf{P}_1, \dots,$ to be just a computable list of every binary predicate of T. We also remark that we could have defined an update to be just a single triple of numbers: all the results of this paper would hold in this case. However, it will be clear in the following that one obtains more efficient programs with our definition of updates: realizers of Post rules will avoid losing precious witnesses.

The consistent union $U_1 \mathcal{U} U_2$ is an non-commutative operation: whenever a triple of U_1 and a triple of U_2 are inconsistent, we arbitrarily keep the triple of U_1 and we reject the triple of U_2, therefore for some U_1, U_2 we have $U_1 \mathcal{U} U_2 \neq U_2 \mathcal{U} U_1$. $\mathcal{U}$ is a "learning strategy", a way of selecting a consistent subset of $U_1 \cup U_2$, such that $U_1 \mathcal{U} U_2 = \emptyset \implies U_1 = U_2 = \emptyset$. Any operator $\mathcal{U}$ selecting a consistent subset of $U_1 \cup U_2$ and satisfying $U_1 \mathcal{U} U_2 = \emptyset \implies U_1 = U_2 = \emptyset$ would produce an alternative Realizability Semantics.

3.2. The System $\mathcal{T}$

$\mathcal{T}$ is formally described in figure 1. Terms of the form $\mathsf{if}_A\, t_1\, t_2\, t_3$ will be written in the more legible form $\mathsf{if}\ t_1\ \mathsf{then}\ t_2\ \mathsf{else}\ t_3$. For every update $U \in \mathbb{U}$, we assume having in $\mathcal{T}$ a constant $\overline{U} : \mathtt{U}$, where $\mathtt{U}$ is a new base type representing $\mathbb{U}$. We write $\varnothing$ for $\overline{\emptyset}$. In $\mathcal{T}$, there are four operations involving updates (see figure 1):

1. The first operation is denoted by the constant $\mathsf{is} : \mathtt{U} \to \mathtt{N}^2 \to \mathtt{Bool}$. is takes as arguments an update constant $\overline{U}$ and two numerals a, n; it returns $\mathtt{True}$ if $(a, n, m) \in U$ for some $m \in \mathtt{N}$ (that is, if the pair (a, n) is in the domain of the partial map U); it returns $\mathtt{False}$ otherwise.

2. The second operation is denoted by the constant $\mathsf{get} : \mathtt{U} \to \mathtt{N}^2 \to \mathtt{N}$. get takes as arguments an update constant $\overline{U}$ and two numerals a, n; it returns m if $(a, n, m) \in U$ for some $m \in \mathtt{N}$ (that is, if (a, n) belongs to the domain of the partial function U);

it returns 0 otherwise.

3. The third operation is denoted by the constant $\mathsf{mkupd} : \mathtt{N}^3 \to \mathtt{U}$. mkupd takes as arguments three numerals a, n, m and transforms them into (the constant coding in $\mathcal{T}$) the update $\{(a, n, m)\}$.

4. The forth operation is denoted by the constant $\Cup : \mathtt{U}^2 \to \mathtt{U}$. $\Cup$ takes as arguments two update constants and returns the update constant denoting their consistent union.

We observe that the constants $\mathsf{is}, \mathsf{get}, \mathsf{mkupd}$ are just syntactic sugar and may be avoided by coding finite partial functions into natural numbers; their behaviour even does not depend on the enumeration $\mathsf{P}_0, \mathsf{P}_1, \ldots$ of binary predicates, since the updates in the language of $\mathcal{T}$ are not assumed to be sound. System $\mathcal{T}$ may thus be coded in Gödel's T.

System $\mathcal{T}$ is obtained from system T adding a new atomic type and new operations on it. The following definition formalizes what has been done in extending T to $\mathcal{T}$, and it useful for defining arbitrary extensions of $\mathcal{T}$ with arbitrary maps over natural numbers. We shall need such extensions when we add the non-computable map Φ to $\mathcal{T}$.

Definition 2 (Functional set of rules). *Let C be any set of constants, each one of some type $A_1 \to \ldots \to A_n \to A$, for some $A_1, \ldots, A_n, A \in \{\mathtt{Bool}, \mathtt{N}, \mathtt{U}\}$. We say that $\mathcal{R}$ is a* functional set of reduction rules *for C if $\mathcal{R}$ consists, for all $c \in C$ and all $a_1 : A_1, \ldots, a_n : A_n$ closed normal terms of $\mathcal{T}$, of exactly one rule $ca_1 \ldots a_n \mapsto a$, for some closed normal term $a : A$ of $\mathcal{T}$.*

Any extension of $\mathcal{T}$ with constants and even non-computable functional sets of rules, is strongly normalizing and has the uniqueness-of-normal-form property.

Theorem 4. *Assume that $\mathcal{R}$ is a functional set of reduction rules for C (def. 2). Then $\mathcal{T} + C + \mathcal{R}$ enjoys strong normalization and weak-Church-Rosser (uniqueness of normal forms) for all closed terms of atomic types.*

Proof. As in [3]

The following normal form theorem also holds.

Lemma 5 (Normal Form Property for $\mathcal{T} + C + \mathcal{R}$). *Assume that $\mathcal{R}$ is a functional set of reduction rules for C. Assume A is either an atomic type or a product type. Then any closed normal term $t \in \mathcal{T}$ of type A is: a numeral $n : \mathtt{N}$, or a boolean $\mathtt{True}, \mathtt{False} : \mathtt{Bool}$, or an update constant $\overline{U} : \mathtt{U}$, or a constant of type A, or a pair $\langle u, v \rangle : B \times C$.*

Proof. As in [3].

In section §2 we made use of the fact that every instance of EM_1 (Excluded Middle over all Σ^1_0-formulas) can be proved from the Excluded Middle over Kleene's predicate.

Definition 3 (Kleene's Predicate $\mathscr{T}$). *With $\mathscr{T} : \mathtt{N}^3 \to \mathtt{N}$ we denote a predicate of Gödel's T representing Kleene's predicate (see e.g., Odifreddi [26]). That is, for any numerals n, m, l, $\mathscr{T}nml = \mathtt{True}$ if and only if the n-th partial recursive function is defined on argument m and l codes a computation proving it.*

Figure 1: the extension $\mathcal{T}$ of Gödel's system T.

Types

$$\sigma, \tau ::= \mathtt{N} \mid \mathtt{Bool} \mid \mathtt{U} \mid \sigma \to \tau \mid \sigma \times \tau$$

Constants

$$c ::= \mathsf{R}_\tau \mid \mathsf{if}_\tau \mid 0 \mid \mathsf{S} \mid \mathtt{True} \mid \mathtt{False} \mid \mathsf{is} \mid \mathsf{get} \mid \mathsf{mkupd} \mid \Cup \mid \overline{U}\ (\forall U \in \mathbb{U})$$

Terms

$$t, u ::= c \mid x^\tau \mid tu \mid \lambda x^\tau u \mid \langle t, u\rangle \mid \pi_0 u \mid \pi_1 u$$

Typing Rules for Variables and Constants

$$\begin{aligned}
x^\tau &: \tau \\
0 &: \mathtt{N} \\
\mathsf{S} &: \mathtt{N} \to \mathtt{N} \\
\mathtt{True} &: \mathtt{Bool} \\
\mathtt{False} &: \mathtt{Bool} \\
\overline{U} &: \mathtt{U} \text{ (for every } U \in \mathbb{U}) \\
\Cup &: \mathtt{U} \to \mathtt{U} \to \mathtt{U} \\
\mathsf{is} &: \mathtt{U} \to \mathtt{N} \to \mathtt{N} \to \mathtt{Bool} \\
\mathsf{get} &: \mathtt{U} \to \mathtt{N} \to \mathtt{N} \to \mathtt{N} \\
\mathsf{mkupd} &: \mathtt{N} \to \mathtt{N} \to \mathtt{N} \to \mathtt{U} \\
\mathsf{if}_\tau &: \mathtt{Bool} \to \tau \to \tau \to \tau \\
\mathsf{R}_\tau &: \tau \to (\mathtt{N} \to (\tau \to \tau)) \to \mathtt{N} \to \tau
\end{aligned}$$

Typing Rules for Composed Terms

$$\frac{t : \sigma \to \tau \qquad u : \sigma}{tu : \tau} \qquad\qquad \frac{u : \tau}{\lambda x^\sigma u : \sigma \to \tau}$$

$$\frac{u : \sigma \qquad t : \tau}{\langle u, t\rangle : \sigma \times \tau} \qquad\qquad \frac{u : \tau_0 \times \tau_1}{\pi_i u : \tau_i}\ i \in \{0, 1\}$$

Reduction Rules All the usual reduction rules for simply typed lambda calculus (see Girard [16]) plus the rules for recursion, if-then-else and projections

$$\mathsf{R}_\tau uv0 \mapsto u \qquad \mathsf{R}_A uv\mathsf{S}(t) \mapsto vt(\mathsf{R}_\tau uvt)$$

$$\mathsf{if}_\tau\, \mathtt{True}\, u\, v \mapsto u \qquad \mathsf{if}_\tau\, \mathtt{False}\, u\, v \mapsto v \qquad \pi_i \langle u_0, u_1\rangle \mapsto u_i, i = 0, 1$$

plus the following ones, assuming a, n, m be numerals:

$$\mathsf{is}\,\overline{U}\, a\, n \mapsto \begin{cases} \mathtt{True} & \text{if } \exists m.\ (a, n, m) \in U \\ \mathtt{False} & \text{otherwise} \end{cases}$$

$$\mathsf{get}\,\overline{U}\, a\, n \mapsto \begin{cases} m & \text{if } \exists m.\ (a, n, m) \in U \\ 0 & \text{otherwise} \end{cases}$$

$$\overline{U}_1 \Cup \overline{U}_2 \mapsto \overline{U_1 \mathcal{U} U_2}$$

$$\mathsf{mkupd}\, a\, n\, m \mapsto \overline{\{(a, n, m)\}}$$

Figure 1: the extension $\mathcal{T}$ of Gödel's system T

3.3. The System $\mathcal{T}_{\textit{Class}}$

We now define a classical extension of $\mathcal{T}$, that we call $\mathcal{T}_{\text{Class}}$, with a constant symbol $\Phi : \mathtt{N}^2 \to \mathtt{N}$ denoting a non-computable map of the same Turing degree of an oracle for the Halting problem. We shall use the elements of $\mathcal{T}_{\text{Class}}$ to represent non-computable realizers.

Definition 4 (The System $\mathcal{T}_{\text{Class}}$). *Define $\mathcal{T}_{\textit{Class}} = \mathcal{T} + \Phi$, where $\Phi : \mathtt{N}^2 \to \mathtt{N}$ is a new constant symbol.*

For every numeral a, Φa – which we shall denote with Φ_a – represents a *Skolem function* for the formula $\exists y^{\mathtt{N}}\, \mathsf{P}_a xy$, taking as argument a number x and returning some y such that $\mathsf{P}_a xy$ if any exists, and an arbitrary value otherwise. There is no set of computable reduction rules for the constant Φ, and therefore no set of computable reduction rules for $\mathcal{T}_{\text{Class}}$.

Each (in general, non-computable) term $t \in \mathcal{T}_{\text{Class}}$ is associated to a set $\{t[s] \mid s \in \mathcal{T}, s : \mathtt{N}^2 \to \mathtt{N}\} \subseteq \mathcal{T}$ of computable terms we call its "approximations", one for each term $s : \mathtt{N}^2 \to \mathtt{N}$ of $\mathcal{T}$, which is thought as a computable approximation of the oracle Φ.

Definition 5 (Approximation at state s). *We define:*

1. *A* state *is a closed term of type $\mathtt{N}^2 \to \mathtt{N}$ of $\mathcal{T}$.*
2. *Assume $t \in \mathcal{T}_{\textit{Class}}$ and s is a state. The "approximation of t at state s" is the term $t[s]$ of $\mathcal{T}$ obtained from t by replacing each constant Φ with s.*

We interpret any $t[s] \in \mathcal{T}$ as a learning process evaluated with respect to the information taken from an approximation s of Φ. Here we consider an approximation of Φ to be an arbitrary term $s : \mathtt{N}^2 \to \mathtt{N}$; s may be correctly in agreement with Φ on some arguments, but wrong on other ones. Consequently, we are going to consider the set of (a, n) such that $\mathsf{P}_a n s_a(n) = \mathtt{True}$ as the real "domain" of s (where $s_a(n)$ denotes san). We are also going to define a term $\oplus$, which takes as argument a term $f : \mathtt{N}^2 \to \mathtt{N}$ and an update $\overline{U}$, and changes the values of f according to U. This is the fundamental operation of our computational model: realizers correct wrong oracle approximations with new correct values that they have previously learned and stored in the updates. Last, using Φ, we are going to define for every numeral a the oracle X_a, which takes as argument a numeral n and returns a guess for the truth value of $\exists y^{\mathtt{N}}\, \mathsf{P}_a ny$.

Definition 6 (Domain, Updates of Functions, Oracle X_a). *We define:*

1. *If s is a state, we denote with $\mathsf{dom}(s)$ the set of pairs of numerals (a, n) such that $\mathsf{P}_a n s_a(n) = \mathtt{True}$.*

2. *We define a term $\oplus : (\mathtt{N}^2 \to \mathtt{N}) \to \mathtt{U} \to (\mathtt{N}^2 \to \mathtt{N})$ as follows:*

$$\oplus := \lambda f^{\mathtt{N}^2 \to \mathtt{N}} \lambda u^{\mathtt{U}} \lambda x^{\mathtt{N}} \lambda y^{\mathtt{N}} \ \mathsf{if}\ (\mathsf{is}\, u\, x\, y)\ \mathsf{then}\ (\mathsf{get}\, u\, x\, y)\ \mathsf{else}\ fxy$$

   We will write $t_1 \oplus t_2$ in place of $\oplus t_1 t_2$.

3. *For every numeral a, we define a term $\mathsf{X}_a : \mathtt{N} \to \mathtt{Bool}$ as follows:*

$$\mathsf{X}_a := \lambda x^{\mathtt{N}}\ \mathsf{P}_a x(\Phi_a x)$$

We introduce now a notion of convergence for families of terms $\{t[s_i]\}_{i\in\mathbb{N}} \subseteq \mathcal{T}$, defined by some $t \in \mathcal{T}_{\text{Class}}$ and indexed over a set $\{s_i\}_{i\in\mathbb{N}}$ of states. Informally, "t convergent" means that the normal form of $t[s]$ eventually stops changing when the approximation s_i of Φ gets better and better. If s and r are states, we formalize what it means that r is at least as good an approximation as s by defining:

$$s \leq r \iff \forall a, n.\ s_a(n) \neq r_a(n) \implies (a, n) \notin \mathsf{dom}(s) \wedge (a, n) \in \mathsf{dom}(r)$$

Intuitively, if $s \leq r$, then r can be obtained by changing some of the values of s that make s a wrong approximation of Φ. We say that a sequence $\{s_i\}_{i\in\mathbb{N}}$ of states is a weakly increasing chain of states (is w.i. for short), if $s_i \leq s_{i+1}$ for all $i \in \mathbb{N}$.

Definition 7 (Convergence). *Assume that $\{s_i\}_{i\in\mathbb{N}}$ is a w.i. sequence of states, and $u \in \mathcal{T}_{\mathit{Class}}$.*

1. *u converges in $\{s_i\}_{i\in\mathbb{N}}$ if $\exists i \in \mathbb{N}. \forall j \geq i.\ u[s_j] = u[s_i]$ in $\mathcal{T}$.*

2. *u converges if u converges in every w.i. sequence of states.*

We remark that if u is convergent, we do not ask that u is convergent to the *same* value on *all* w.i. chain of oracle approximations. The limit value of u may depend on the information contained in the particular chain from which u gets the knowledge. The chain of approximations, in turn, is selected by the particular definition we use for the "learning strategy" $\mathcal{U}$. Different "learning strategies" may produce different limit values.

Theorem 6 (Convergence Theorem). *Assume $t \in \mathcal{T}_{\mathit{Class}}$ is a closed term of atomic type A ($A \in \{\mathtt{Bool}, \mathtt{N}, \mathtt{U}\}$). Then t is convergent.*

Proof. As in [3].

Remark 1. The idea of the proof of theorem 6 corresponds exactly to the intuition that during any computation, the oracle Φ is consulted a finite number of times and hence asked for a finite number of values. When the approximation s_n of Φ is great enough, we can substitute Φ with s_n and we obtain the same oracle values and hence the same results.

4. An Interactive Learning-Based Notion of Realizability for $\mathsf{HA}^\omega + \mathsf{EM}_1 + \mathsf{SK}_1$

In this section we introduce a learning-based notion of realizability for $\mathsf{HA}^\omega + \mathsf{EM}_1 + \mathsf{SK}_1$, Heyting Arithmetic in all finite types (see e.g. Troelstra [31]) plus Excluded Middle scheme for all Σ^0_1-formulas:

$$\mathsf{EM}_1 := \forall x^{\mathtt{N}}.\ \exists y^{\mathtt{N}} \mathsf{P}_a x y \vee \forall y^{\mathtt{N}} \neg \mathsf{P}_a x y$$

and Skolem axioms for all Σ^0_1-formulas:

$$\mathsf{SK}_1 := \forall x^{\mathtt{N}} \forall y^{\mathtt{N}}.\ \mathsf{P}_a x y \to \mathsf{P}_a x \Phi_a(x)$$

then we prove our main Theorem, the Adequacy Theorem: *"if a closed arithmetical formula is provable in $\mathsf{HA}^\omega + \mathsf{EM}_1 + \mathsf{SK}_1$, then it is realizable".*

We first define the formal system $\mathsf{HA}^{\omega}+\mathsf{EM}_1+\mathsf{SK}_1$. We represent atomic predicates of $\mathsf{HA}^{\omega}+\mathsf{EM}_1+\mathsf{SK}_1$ with (in general, non-computable) closed terms of $\mathcal{T}_{\text{Class}}$ of type $\mathtt{Bool}$. Terms of $\mathsf{HA}^{\omega}+\mathsf{EM}_1+\mathsf{SK}_1$ may include the function symbol Φ, with Φ_a denoting the Skolem function for $\exists y^{\mathtt{N}}\mathsf{P}_a xy$. We assume having in Gödel's T some terms $\Rightarrow_{\mathtt{Bool}}: \mathtt{Bool} \to \mathtt{Bool} \to \mathtt{Bool}, \neg_{\mathtt{Bool}} : \mathtt{Bool} \to \mathtt{Bool}, \vee_{\mathtt{Bool}} : \mathtt{Bool} \to \mathtt{Bool} \to \mathtt{Bool} \ldots$, implementing boolean connectives. If $t_1, \ldots, t_n, t \in \mathsf{T}$ have type $\mathtt{Bool}$ and are made from free variables all of type $\mathtt{Bool}$, using boolean connectives, we say that t is a tautological consequence of $t_1, \ldots, t_n$ in T (a tautology if $n = 0$) if all boolean assignments making $t_1, \ldots, t_n$ equal to $\mathtt{True}$ in T also make t equal to $\mathtt{True}$ in T.

4.1. Language of $\mathsf{HA}^{\omega}+\mathsf{EM}_1+\mathsf{SK}_1$

We now define the language of the arithmetical theory $\mathsf{HA}^{\omega}+\mathsf{EM}_1+\mathsf{SK}_1$.

Definition 8 (Language of $\mathsf{HA}^{\omega}+\mathsf{EM}_1+\mathsf{SK}_1$). *The language $\mathcal{L}_{\textit{Class}}$ of $\mathsf{HA}^{\omega}+\mathsf{EM}_1+\mathsf{SK}_1$ is defined as follows.*

1. *The terms of $\mathcal{L}_{\textit{Class}}$ are all $t \in \mathcal{T}_{\textit{Class}}$.*

2. *The atomic formulas of $\mathcal{L}_{\textit{Class}}$ are all $Q \in \mathcal{T}_{\textit{Class}}$ such that $Q : \mathtt{Bool}$.*

3. *The formulas of $\mathcal{L}_{\textit{Class}}$ are built from atomic formulas of $\mathcal{L}_{\textit{Class}}$ by the connectives $\vee, \wedge, \to \forall, \exists$ as usual, with quantifiers possibly ranging over variables $x^{\tau}, y^{\tau}, z^{\tau}$ of arbitrary finite type τ of $\mathcal{T}$.*

We denote with $\perp$ the atomic formula $\mathtt{False}$. If P is an atomic formula of $\mathcal{L}_{\text{Class}}$ in the free variables $x_1^{\tau_1}, \ldots, x_n^{\tau_n}$ and $t_1 : \tau_1, \ldots, t_n : \tau_n$ are terms of $\mathcal{L}_{\text{Class}}$, with $P(t_1, \ldots, t_n)$ we shall denote the atomic formula $P[t_1/x_1, \ldots, t_n/x_n]$.

We defined $\Rightarrow_{\mathtt{Bool}}: \mathtt{Bool}, \mathtt{Bool} \to \mathtt{Bool}$ as a term implementing implication, therefore, to be accurate, formulas of the form $\mathsf{P}_a(t,u) \Rightarrow_{\mathtt{Bool}} \mathsf{P}_a(t, \Phi_a t)$ are not an implication between two atomic formulas, but they are equal to the single atomic formula Q, where

$$Q := \Rightarrow_{\mathtt{Bool}} (\mathsf{P}_a tu)(\mathsf{P}_a t(\Phi_a t))$$

Any atomic formula A of $\mathcal{L}_{\text{Class}}$ is a boolean term of $\mathcal{T}_{\text{Class}}$, therefore for any $s : \mathtt{N}^2 \to \mathtt{N}$ of $\mathcal{T}$ we may form the "approximation" $A[s] : \mathtt{Bool}, A[s] \in \mathcal{T}$ of A. In $A[s]$ we replace the Skolem function Φ we have in A by its approximation s.

From now onwards, for every pair of terms t_1, t_2 of system $\mathcal{T}$, we shall write $t_1 = t_2$ if they are the same term modulo the equality rules corresponding to the reduction rules of system $\mathcal{T}$ (equivalently, if they have the same normal form).

4.2. Interactive (or Learning-Based) Realizability

For every formula A of $\mathcal{L}_{\text{Class}}$, we are now going to define what type $|A|$ a realizer of A must have.

Definition 9 (Types for realizers). *For each formula A of $\mathcal{L}_{\textit{Class}}$ we define a type $|A|$ of $\mathcal{T}_{\textit{Class}}$ by induction on A:*

1. $|P| = \mathtt{U}$, *if P is atomic,*

2. $|A \wedge B| = |A| \times |B|$,

3. $|A \vee B| = \mathtt{Bool} \times (|A| \times |B|)$,

4. $|A \to B| = |A| \to |B|$,

5. $|\forall x^\tau A| = \tau \to |A|$,

6. $|\exists x^\tau A| = \tau \times |A|$.

Let now $\mathsf{p}_0 := \pi_0 : \sigma_0 \times (\sigma_1 \times \sigma_2) \to \sigma_0$, $\mathsf{p}_1 := \pi_0\pi_1 : \sigma_0 \times (\sigma_1 \times \sigma_2) \to \sigma_1$ and $\mathsf{p}_2 := \pi_1\pi_1 : \sigma_0 \times (\sigma_1 \times \sigma_2) \to \sigma_2$ be the three canonical projections from $\sigma_0 \times (\sigma_1 \times \sigma_2)$. We define the realizability relation $t \Vdash A$, where $t \in \mathcal{T}_{\text{Class}}$, $A \in \mathcal{L}_{\text{Class}}$ and $t : |A|$.

Definition 10 (Interactive Realizability). *Assume s is a state, t is a closed term of $\mathcal{T}_{\text{Class}}$, $C \in \mathcal{L}_{\text{Class}}$ is a closed formula, and $t : |C|$. We define first the relation $t \Vdash_s C$ by induction and by cases according to the form of C:*

1. *$t \Vdash_s Q$ for some atomic Q if and only if $t[s] = \overline{U}$ implies:*
   - *U is sound and $\mathsf{dom}(U) \cap \mathsf{dom}(s) = \emptyset$*
   - *$U = \varnothing$ implies $Q[s] = \mathtt{True}$*

2. *$t \Vdash_s A \wedge B$ if and only if $\pi_0 t \Vdash_s A$ and $\pi_1 t \Vdash_s B$*

3. *$t \Vdash_s A \vee B$ if and only if either $\mathsf{p}_0 t[s] = \mathtt{True}$ and $\mathsf{p}_1 t \Vdash_s A$, or $\mathsf{p}_0 t[s] = \mathtt{False}$ and $\mathsf{p}_2 t \Vdash_s B$*

4. *$t \Vdash_s A \to B$ if and only if for all u, if $u \Vdash_s A$, then $tu \Vdash_s B$*

5. *$t \Vdash_s \forall x^\tau A$ if and only if for all closed terms $u : \tau$ of $\mathcal{T}$, $tu \Vdash_s A[u/x]$*

6. *$t \Vdash_s \exists x^\tau A$ if and only for some closed term $u : \tau$ of $\mathcal{T}$, $\pi_0 t[s] = u$ and $\pi_1 t \Vdash_s A[u/x]$*

We define $t \Vdash A$ if and only if for all closed $s : \mathtt{N} \to \mathtt{N}$ of $\mathcal{T}$, $t \Vdash_s A$.

Remark 2. The ideas behind the definition of $\Vdash_s$ in the case of $\mathsf{HA} + \mathsf{EM}_1 + \mathsf{SK}_1$ are those we already explained in [3], [1]. The system $\mathsf{HA}^\omega + \mathsf{EM}_1 + \mathsf{SK}_1$ has, w.r.t. the system $\mathsf{HA} + \mathsf{EM}_1 + \mathsf{SK}_1$ considered in our previous papers, a new feature: its quantifiers range over terms of arbitrary finite type, i.e. over the functionals definable in $\mathcal{L}_{\text{Class}}$. These functionals, in general, are not recursive. However, in each particular world/state s what is in general uncomputable becomes computable, since the Skolem function Φ is interpreted by a computable approximation s. Thus, in the state s every term of $\mathcal{L}_{\text{Class}}$ becomes recursive and, in fact, a term of Gödel's system T. This is the reason why in the definition of the realizability relation $\Vdash_s$ all quantifiers range over terms of system T.

The next proposition tells that realizability at state s respects the notion of equality of $\mathcal{T}_{\text{Class}}$ terms, when the latter is relativized to state s. That is, if two terms are equal at the state s, then they realize the same formulas at the state s.

Proposition 1 (Saturation). *If $t_1[s] = t_2[s]$ and $u_1[s] = u_2[s]$, then $t_1 \Vdash_s B[u_1/x]$ if and only if $t_2 \Vdash_s B[u_2/x]$.*

Proof. By straightforward induction on A.

Example 1. The most remarkable feature of our Realizability Semantics is the existence of a realizer for EM_1. Assume that P_a is a predicate of T and define

$$\mathsf{E}_a := \lambda\alpha^{\mathtt{N}}\langle \mathsf{X}_a\alpha,\ \langle \Phi_a\alpha,\ \varnothing\rangle, \lambda n^{\mathtt{N}}\ \mathsf{if}\ \mathsf{P}_a\alpha n\ \mathsf{then}\ \mathsf{mkupd}\, a\,\alpha\, n\ \mathsf{else}\ \varnothing\rangle$$

Indeed E_a realizes its associated instance of EM_1.

Proposition 2 (Realizer E_a of EM_1).

$$\mathsf{E}_a \Vdash \forall x^{\mathtt{N}}.\ \exists y^{\mathtt{N}}\ \mathsf{P}_a(x,y) \vee \forall y^{\mathtt{N}} \neg_{\mathtt{Bool}} \mathsf{P}_a(x,y)$$

Proof. Let m be any numeral. We have

$$\mathsf{E}_a m = \langle \mathsf{X}_a m,\ \langle \Phi_a m,\ \varnothing\rangle, \lambda n^{\mathtt{N}}\ \mathsf{if}\ \mathsf{P}_a m n\ \mathsf{then}\ \mathsf{mkupd}\, a\, m\, n\ \mathsf{else}\ \varnothing\rangle$$

and we want to prove that

$$\mathsf{E}_a m \Vdash_s \exists y^{\mathtt{N}}\ \mathsf{P}_a(m,y) \vee \forall y^{\mathtt{N}} \neg_{\mathtt{Bool}} \mathsf{P}_a(m,y)$$

We have $\mathsf{p}_0\mathsf{E}_a m = \mathsf{X}_a m = \mathsf{P}_a(m, \Phi_a(m))$. There are two cases.

1. $\mathsf{X}_a m[s] = \mathtt{True}$. Let $n = s_a(m)$. Then $\mathsf{P}_a(m,n) = \mathtt{True}$ and we have to prove

   $$\mathsf{p}_1\mathsf{E}_a m \Vdash_s \exists y^{\mathtt{N}}\ \mathsf{P}_a(m,y)$$

   By definition

   $$\mathsf{p}_1\mathsf{E}_a m = \langle \Phi_a m, \varnothing\rangle$$

   Thus

   $$\pi_0(\mathsf{p}_1\mathsf{E}_P m)[s] = \pi_0\langle s_a(m), \varnothing\rangle = n$$

   and

   $$\pi_1(\mathsf{p}_1\mathsf{E}_a m) \Vdash_s \mathsf{P}_a(m,n)$$

   because $\mathsf{P}_a(m,n) = \mathtt{True}$. We conclude

   $$\mathsf{p}_1\mathsf{E}_a m \Vdash_s \exists y^{\mathtt{N}}\ P(m,y)$$

2. $\mathsf{X}_a m[s] = \mathtt{False}$. We have to prove

   $$\mathsf{p}_2\mathsf{E}_a m = \lambda n^{\mathtt{N}}\ \mathsf{if}\ \mathsf{P}_a m n\ \mathsf{then}\ \mathsf{mkupd}\, a\, m\, n\ \mathsf{else}\ \varnothing\ \Vdash_s \forall y^{\mathtt{N}} \neg_{\mathtt{Bool}} \mathsf{P}_a(m,y)$$

   i.e. that given any numeral n

   $$\mathsf{if}\ \mathsf{P}_a m n\ \mathsf{then}\ \mathsf{mkupd}\, a\, m\, n\ \mathsf{else}\ \varnothing \Vdash_s \neg_{\mathtt{Bool}} \mathsf{P}_a(m,n)$$

If $\mathsf{P}_a(m,n) = \mathtt{False}$, the thesis follows since $\neg_{\mathtt{Bool}}\mathsf{P}_a(m,n) = \mathtt{True}$. If $\mathsf{P}_a(m,n) = \mathtt{True}$, then

$$\mathsf{if}\ \mathsf{P}_a mn\ \mathsf{then}\ \mathsf{mkupd}\, a\, m\, n\ \mathsf{else}\ \varnothing = \{(a,m,n)\} \Vdash_s \neg_{\mathtt{Bool}}\mathsf{P}_a(m,n)$$

since $\mathsf{P}_a(m, s_a(m)) = \mathtt{False}$ and thus $\mathsf{dom}(\{(a,m,n)\}) = \{(a,m)\}$ and $(a,m) \notin \mathsf{dom}(s)$.

We now prove that if we start from any term $s_0 : \mathtt{N}^2 \to \mathtt{N}$ of $\mathcal{T}$ and we repeatedly apply any atomic realizer $t : \mathtt{U}$ of $\mathcal{T}_{\text{Class}}$, we obtain a "zero" of t, that is a term $s_n : \mathtt{N}^2 \to \mathtt{N}$ of $\mathcal{T}$ such that $t[s_n] = \varnothing$. We interpret this by saying that any atomic realizer t represents a terminating learning process.

Theorem 7 (Zero Theorem). *Let Q be an atomic formula of $\mathcal{L}_{\text{Class}}$ and suppose $t \Vdash Q$. Let $s : \mathtt{N}^2 \to \mathtt{N}$ be a closed term of $\mathcal{T}$. Define, by induction on n, a sequence $\{s_n\}_{n\in\mathbb{N}}$ of terms such that:*

$$s_0 := s$$
$$s_{n+1} := s_n \oplus t[s_n] \overset{def\ 6}{=} \lambda x^{\mathtt{N}} \lambda y^{\mathtt{N}}\ \mathsf{if}\ (\mathsf{is}\, t[s_n]\, x\, y)\ \mathsf{then}\ (\mathsf{get}\, t[s_n]\, x\, y)\ \mathsf{else}\ s_n(x,y)$$

Then, there exists a n such that $t[s_n] = \varnothing$.

Proof. We first prove that $s_0, s_1, s_2, \dots$ is a weakly increasing chain. Suppose $s_i(a,n) \neq s_{i+i}(a,n)$: we have to prove that $(a,n) \in \mathsf{dom}(s_{i+1})$ and $(a,n) \notin \mathsf{dom}(s_i)$. By definition of s_{i+1}, if it were $\mathsf{is}\, t[s_i]\, a\, n = \mathtt{False}$, then we would have $s_i(a,n) = s_{i+i}(a,n)$, contradiction. Thus, $\mathsf{is}\, t[s_i]\, a\, n = \mathtt{True}$, and if we choose an update U such that $\overline{U} = t[s_i]$, we have:

$$\mathsf{is}\, \overline{U}\, a\, n = \mathtt{True}$$

that is, $(a,n) \in \mathsf{dom}(U)$, and for some m, $(a,n,m) \in U$. By definition of $t \Vdash_{s_i} Q$ we deduce that U is sound and $\mathsf{dom}(s_i) \cap \mathsf{dom}(U) = \emptyset$. From $\mathsf{dom}(s_i) \cap \mathsf{dom}(U) = \emptyset$ and $(a,n) \in \mathsf{dom}(U)$ we obtain $(a,n) \notin \mathsf{dom}(s_i)$. From U is sound and $(a,n,m) \in U$ we obtain $\mathsf{P}_a nm = \mathtt{True}$. By definition,

$$s_{i+1}(a,n) = \mathsf{get}\, t[s_i]\, a\, n = \mathsf{get}\, \overline{U}\, a\, n = m$$

Therefore, $s_{i+1}(a,n) = m$ and by definition 6 of dom, we have that $(a,n) \in \mathsf{dom}(s_{i+1})$. We conclude that $s_0, s_1, s_2, \dots$ is weakly increasing.
Now, by theorem 6, t converges over the chain $\{s_i\}_{i\in\mathbb{N}}$: there exists $k \in \mathbb{N}$ such that for every $j \geq k$, $t[s_j] = t[s_k]$. By choice of k

$$\begin{aligned} s_{k+1} \oplus t[s_{k+1}] &= (s_k \oplus t[s_k]) \oplus t[s_{k+1}] \\ &= (s_k \oplus t[s_k]) \oplus t[s_k] \\ &= s_k \oplus t[s_k] \\ &= s_{k+1} \end{aligned}$$

and hence it must be that $t[s_k] = \varnothing$, which is the thesis.

The Zero Theorem could be expressed, in an equivalent way, as a fixed point result, but we skip this reformulation for sake of brevity. As usual for a realizability interpretation, we may extract from any realizer $t \Vdash \forall x^{\sigma} \exists y^{\tau} Pxy$, with $P : \sigma \to \tau \to \texttt{Bool}$ closed term of system $\mathcal{T}$, some recursive map f from the set of terms of type σ to the set of terms of type τ, such that $Puf(u) = \texttt{True}$ for all $u : \sigma$.

Theorem 8 (Program Extraction via Learning Based Realizability). *Let t be a term of $\mathcal{T}_{\mathit{Class}}$ and suppose that $t \Vdash \forall x^{\sigma} \exists y^{\tau} Pxy$, with $P : \sigma \to \tau \to \texttt{Bool}$ closed term of system $\mathcal{T}$. Then:*

1. *From t one can effectively define a recursive function f such that for every closed term $u : \sigma$ of system T, $f(u) : \tau$ is a term of system $\mathcal{T}$ such that $Pu(f(u)) = \texttt{True}$.*

2. *If $\sigma \in \{\texttt{N}, \texttt{N} \to \texttt{N}\}$, then f can be represented in system $\mathcal{T}$.*

3. *If $\sigma \notin \{\texttt{N}, \texttt{N} \to \texttt{N}\}$, then f can be represented in system $\mathcal{T}$ plus Spector's bar recursion (see Spector [30]).*

Proof. 1. Let

$$v := \lambda m^{\sigma}\ \pi_1(tm)$$

v is of type $\sigma \to \texttt{U}$. Since for every closed $u : \sigma$ of $\mathcal{T}$

$$vu \Vdash Pu\pi_0(tu)$$

by the zero theorem 7, there exists a recursive function zero from the set of type-σ terms of system $\mathcal{T}$ to the set of type-$\texttt{N}^2 \to \texttt{N}$ terms of $\mathcal{T}$ such that $vu[\mathsf{zero}(u)] = \varnothing$ for every closed $u : \sigma$ of $\mathcal{T}$. Define the function

$$f := w \mapsto \pi_0(tw)[\mathsf{zero}(w)]$$

and fix a closed term $u : \sigma$ of $\mathcal{T}$. By unfolding the definition of realizability with respect to $\mathsf{zero}(u)$, we have that

$$tu \Vdash_{\mathsf{zero}(u)} \exists y^{\tau} Puy$$

and hence

$$\pi_1(tu) \Vdash_{\mathsf{zero}(u)}\ Pu(f(u))$$

that is to say

$$vu[\mathsf{zero}(u)] = \varnothing \implies Pu(f(u)) = \texttt{True}$$

and therefore

$$Pu(f(u)) = \texttt{True}$$

which is the thesis.

2. The fact that f can be represented in system $\mathcal{T}$ follows by the methods of Aschieri [5]. In particular, by theorem 12 of [5], the function zero is representable in system $\mathcal{T}$ when $\sigma = \texttt{N}$, because $\lambda m^{\sigma} \lambda g^{\texttt{N} \to \texttt{N}} vm[g]$ is a numerable collection of update procedures (see Avigad [6], Aschieri [5]). A straightforward generalization of the aforementioned theorem 12 of [5] –taking care of collection of update procedures indexed by terms of type $\texttt{N} \to \texttt{N}$ – extends the result for $\sigma = \texttt{N} \to \texttt{N}$.

3. See Aschieri [3], [4] for a proof that the function zero is representable in system $\mathcal{T}$ plus bar recursion.

Remark 3. The function f described in theorem 8, point 1, reduces the problem of finding a witness for the formula $\exists x^\tau Pux$ to the problem of computing a zero of the atomic realizer

$$vu := \pi_1(tu)$$

This latter problem is solved by f by computing the sequence

$$s_0 := s$$
$$s_{n+1} := s_n \oplus vu[s_n]$$

until a n is found such that $vu[s_n] = \varnothing$. The translation of f in a term of system $\mathcal{T}$, which exists by theorem 8, point 2, yields the very same algorithm. The crucial fact is that the number n can be computed directly in system $\mathcal{T}$ and thus the iteration that allows to compute s_n can be expressed by the primitive recursor of $\mathcal{T}$. For details see [3, 5].

4.3. Curry-Howard Correspondence for $\mathsf{HA}^\omega + \mathsf{EM}_1 + \mathsf{SK}_1$

In figure 2, we define a standard natural deduction system for $\mathsf{HA}^\omega + \mathsf{EM}_1 + \mathsf{SK}_1$ (see [29], for example) together with a term assignment in the spirit of Curry-Howard correspondence for classical logic.

We replace purely universal axioms (i.e., Π^0_1-axioms) with Post rules, which are inferences of the form

$$\frac{\Gamma \vdash A_1 \; \Gamma \vdash A_2 \; \cdots \; \Gamma \vdash A_n}{\Gamma \vdash A}$$

where $A_1, \ldots, A_n, A$ are atomic formulas of $\mathcal{L}_{\text{Class}}$ such that for every substitution $\sigma = [t_1/x_1, \ldots, t_k/x_k \; s/\Phi]$ of closed terms $t_1, \ldots, t_k$ of $\mathcal{T}$ and closed $s : \mathtt{N}^2 \to \mathtt{N}$ of $\mathcal{T}$, $A_1\sigma = \ldots = A_n\sigma = \mathtt{True}$ implies $A\sigma = \mathtt{True}$. Let now $\mathsf{eq} : \mathtt{N}^2 \to \mathtt{Bool}$ a term of Gödel's system T representing equality between natural numbers. Among the Post rules, we have the Peano axioms

$$\frac{\Gamma \vdash \mathsf{eq}\ \mathsf{S}(x)\,\mathsf{S}(y)}{\Gamma \vdash \mathsf{eq}\ x\,y} \qquad \frac{\Gamma \vdash \mathsf{eq}\ 0\,\mathsf{S}(x)}{\Gamma \vdash \bot}$$

and axioms of equality

$$\frac{}{\Gamma \vdash \mathsf{eq}\ x\,x} \qquad \frac{\Gamma \vdash \mathsf{eq}\,x\,y \quad \Gamma \vdash \mathsf{eq}\,y\,z}{\Gamma \vdash \mathsf{eq}\ x\,z} \qquad \frac{\Gamma \vdash A(x) \quad \Gamma \vdash \mathsf{eq}\,x\,y}{\Gamma \vdash A(y)}$$

and for every A_1, A_2 such that $A_1 = A_2$ is an equation of Gödel's system T (equivalently, A_1, A_2 have the same normal form in T), we have the rule

$$\frac{\Gamma \vdash A_1}{\Gamma \vdash A_2}$$

We add also have a Post rule

$$\frac{\Gamma \vdash A_1 \; \Gamma \vdash A_2 \; \cdots \; \Gamma \vdash A_n}{\Gamma \vdash A}$$

Figure 2: Term Assignment Rules for $\mathsf{HA}^\omega + \mathsf{EM}_1 + \mathsf{SK}_1$

Contexts With Γ we denote contexts of the form $x_1 : A_1, \ldots, x_n : A_n$, with $x_1, \ldots, x_n$ proof variables and $A_1, \ldots, A_n$ formulas of $\mathcal{L}_{\text{Class}}$.

Axioms $\Gamma, x : A \vdash x^{|A|} : A$

Conjunction $\dfrac{\Gamma \vdash u : A \quad \Gamma \vdash t : B}{\Gamma \vdash \langle u, t\rangle : A \wedge B}$ $\qquad \dfrac{\Gamma \vdash u : A \wedge B}{\Gamma \vdash \pi_0 u : A}$ $\qquad \dfrac{\Gamma \vdash u : A \wedge B}{\Gamma \vdash \pi_1 u : B}$

Implication $\dfrac{\Gamma \vdash u : A \to B \quad \Gamma \vdash t : A}{\Gamma \vdash ut : B}$ $\qquad \dfrac{\Gamma, x : A \vdash u : B}{\Gamma \vdash \lambda x^{|A|} u : A \to B}$

Disjunction Intro. $\dfrac{\Gamma \vdash u : A}{\Gamma \vdash \langle \mathtt{True}, u, d^{|B|}\rangle : A \vee B}$ $\qquad \dfrac{\Gamma \vdash u : B}{\Gamma \vdash \langle \mathtt{False}, d^{|A|}, u\rangle : A \vee B}$

Disjunction Elim. $\dfrac{\Gamma \vdash u : A \vee B \quad \Gamma, x : A \vdash w_1 : C \quad \Gamma, x : B \vdash w_2 : C}{\Gamma \vdash \mathsf{if}\ \mathsf{p}_0 u\ \mathsf{then}\ (\lambda x^{|A|} w_1)(\mathsf{p}_1 u)\ \mathsf{else}\ (\lambda x^{|B|} w_2)(\mathsf{p}_2 u) : C}$

Universal Quantification $\dfrac{\Gamma \vdash u : \forall \alpha^\tau A}{\Gamma \vdash ut : A[t/\alpha^\tau]}$ $\dfrac{\Gamma \vdash u : A}{\Gamma \vdash \lambda \alpha^\tau u : \forall \alpha^\tau A}$

where t is a term of $\mathcal{L}_{\text{Class}}$ and $\alpha^{\mathtt{N}}$ does not occur free in any formula B occurring in Γ.

Existential Quantification $\dfrac{\Gamma \vdash u : A[t/\alpha^\tau]}{\Gamma \vdash \langle t, u\rangle : \exists \alpha^\tau . A}$ $\qquad \dfrac{\Gamma \vdash u : \exists \alpha^\tau . A \quad \Gamma, x : A \vdash t : C}{\Gamma \vdash (\lambda \alpha^\tau \lambda x^{|A|}\ t)(\pi_0 u)(\pi_1 u) : C}$

where α^τ is not free in C nor in any formula B occurring in Γ.

Induction $\dfrac{\Gamma \vdash u : A(0) \quad \Gamma \vdash v : \forall \alpha^{\mathtt{N}} . A(\alpha) \to A(\mathsf{S}(\alpha))}{\Gamma \vdash \lambda \alpha^{\mathtt{N}} \mathsf{R} u v \alpha : \forall \alpha^{\mathtt{N}} A}$

Post Rules $\dfrac{\Gamma \vdash u_1 : A_1\ \Gamma \vdash u_2 : A_2\ \cdots\ \Gamma \vdash u_n : A_n}{\Gamma \vdash u_1 \Cup u_2 \Cup \cdots \Cup u_n : A}$

where $n > 0$ and $A_1, A_2, \ldots, A_n, A$ are atomic formulas of $\mathcal{L}_{\text{Class}}$, and the rule is a Post rule for equality, for a Peano axiom or for a classical propositional tautology or for booleans.

Post Rules with no Premises $\dfrac{}{\Gamma \vdash \varnothing : A}$

where A is an atomic formula of $\mathcal{L}_{\text{Class}}$ and an axiom of equality or a classical propositional tautology.

EM1 $\dfrac{}{\Gamma \vdash \mathsf{E}_a : \forall x^{\mathtt{N}} .\ \exists y^{\mathtt{N}}\ \mathsf{P}_a(x, y) \vee \forall y^{\mathtt{N}} \neg_{\mathtt{Bool}} \mathsf{P}_a(x, y)}$

SK1 $\dfrac{}{\Gamma \vdash \lambda x^{\mathtt{N}} \lambda y^{\mathtt{N}} \mathsf{if}\ (\mathsf{P}_a x y \Rightarrow_{\mathtt{Bool}} \mathsf{P}_a x(\Phi_a x))\ \mathsf{then}\ \varnothing\ \mathsf{else}\ (\mathsf{mkupd}\, a\, x\, y) : \forall x^{\mathtt{N}} \forall y^{\mathtt{N}} .\ \mathsf{P}_a(x, y) \Rightarrow_{\mathtt{Bool}} \mathsf{P}_a(x, \Phi_a x)}$

Figure 2: Terms Assignement Rules for $\mathsf{HA}^\omega + \mathsf{EM}_1 + \mathsf{SK}_1$

for every classical propositional tautology $A_1 \to \ldots \to A_n \to A$, where for $i = 1, \ldots, n$, A_i, A are atomic formulas obtained as combination of other atomic formulas by the

Gödel's system T boolean connectives. As title of example, we have the rules

$$\frac{\Gamma \vdash \bot}{\Gamma \vdash P} \qquad \frac{\Gamma \vdash B}{\Gamma \vdash A \Rightarrow_{\texttt{Bool}} B} \qquad \frac{\Gamma \vdash A \wedge_{\texttt{Bool}} B}{\Gamma \vdash A}$$

Finally, we have a rule of case reasoning for booleans. For any atomic formula P and any formula $A[P]$ we have:

$$\frac{\Gamma \vdash A[\texttt{True}] \quad \Gamma \vdash A[\texttt{False}]}{\Gamma \vdash A[P]}$$

The connectives $\vee_{\texttt{Bool}}$ and $\vee$ have the same meaning but they are syntactically different: for every atomic formula P, we consider $P \vee_{\texttt{Bool}} \neg_{\texttt{Bool}} P$ an atomic formula and $P \vee \neg_{\texttt{Bool}} P$ a compound formula. $P \vee_{\texttt{Bool}} \neg_{\texttt{Bool}} P$ is an axiom, while we may derive $\mathsf{HA}^\omega \vdash P \vee \neg_{\texttt{Bool}} P$ by case reasoning.

Assume $u_1, \dots, u_n$ are realizers of the assumptions of a Post rule. Then a realizer of the conclusion of a Post rule is of the form $u = u_1 \Cup \cdots \Cup u_n$. In this case, we have n different realizers, whose learning capabilities are put together through a sort of union. In order to prove that u realizes A, assume that $u[s] = \varnothing$, then $u_1[s] = \ldots = u_n[s] = \varnothing$, i.e. all u_i "have nothing to learn". In that case, each u_i must guarantee A_i to be true, and therefore the conclusion of the Post rule is true, because true premises $A_1, \dots, A_n$ spell a true conclusion A. Thus, u realizes A.

If T is any type of $\mathcal{T}$, we denote with d^T a dummy term of type T, defined by $d^{\mathtt{N}} = 0$, $d^{\mathtt{Bool}} = \texttt{False}$, $d^{\mathtt{U}} = \varnothing$, $d^{A \to B} = \lambda z^A . d^B$ (with z^A any variable of type A), $d^{A \times B} = \langle d^A, d^B \rangle$.

We now prove our main theorem, that every theorem of $\mathsf{HA}^\omega + \mathsf{EM}_1 + \mathsf{SK}_1$ is realizable. As usual in adequacy proofs for realizability, we prove a stronger version of the theorem, suitable to be proved by induction on proofs.

Theorem 9 (Adequacy Theorem). *Suppose that $\Gamma \vdash w : A$ in the system $\mathsf{HA}^\omega + \mathsf{EM}_1 + \mathsf{SK}_1$, with $\Gamma = x_1 : A_1, \dots, x_n : A_n$, and that the free variables of the formulas occurring in Γ and A are among $\alpha_1 : \tau_1, \dots, \alpha_k : \tau_k$. For all states s and for all closed terms $r_1 : \tau_1, \dots, r_k : \tau_k$ of system $\mathcal{T}$, if there are terms $t_1, \dots, t_n$ such that*

$$\text{for } i = 1, \dots, n,\ t_i \Vdash_s A_i[r_1/\alpha_1 \cdots r_k/\alpha_k]$$

then

$$w[t_1/x_1^{|A_1|} \cdots t_n/x_n^{|A_n|}\ r_1/\alpha_1 \cdots r_k/\alpha_k] \Vdash_s A[r_1/\alpha_1 \cdots r_k/\alpha_k]$$

Proof. Notation: for any term v and formula B, we denote

$$v[t_1/x_1^{|A_1|} \cdots t_n/x_n^{|A_n|}\ r_1/\alpha_1 \cdots r_k/\alpha_k]$$

with $\overline{v}$ and

$$B[r_1/\alpha_1 \cdots r_k/\alpha_k]$$

with $\overline{B}$. We have $|\overline{B}| = |B|$ for all formulas B. We denote with $=$ the provable equality in $\mathcal{T}_{\text{Class}}$. We proceed by induction on w. Consider the last rule in the derivation of $\Gamma \vdash w : A$:

1. If it is the rule for variables, then for some i, $w = x_i^{|A_i|}$ and $A = A_i$. So $\overline{w} = t_i \Vdash_s \overline{A_i} = \overline{A}$.

2. If it is the $\wedge I$ rule, then $w = \langle u, t\rangle$, $A = B \wedge C$, $\Gamma \vdash u : B$ and $\Gamma \vdash t : C$. Therefore, $\overline{w} = \langle \overline{u}, \overline{t}\rangle$. By induction hypothesis, $\pi_0 \overline{w} = \overline{u} \Vdash_s \overline{B}$ and $\pi_1 \overline{w} = \overline{t} \Vdash_s \overline{C}$; so, by definition, $\overline{w} \Vdash_s \overline{B} \wedge \overline{C} = \overline{A}$.

3. If it is a $\wedge E$ rule, say left, then $w = \pi_0 u$ and $\Gamma \vdash u : A \wedge B$. So $\overline{w} = \pi_0 \overline{u} \Vdash_s \overline{A}$, because $\overline{u} \Vdash_s \overline{A} \wedge \overline{B}$ by induction hypothesis.

4. If it is the $\rightarrow E$ rule, then $w = ut$, $\Gamma \vdash u : B \rightarrow A$ and $\Gamma \vdash t : B$. So $\overline{w} = \overline{u}\overline{t} \Vdash_s \overline{A}$, for $\overline{u} \Vdash_s \overline{B} \rightarrow \overline{A}$ and $\overline{t} \Vdash_s \overline{B}$ by induction hypothesis.

5. If it is the $\rightarrow I$ rule, then $w = \lambda x^{|B|} u$, $A = B \rightarrow C$ and $\Gamma, x : B \vdash u : C$. Suppose now that $t \Vdash_s \overline{B}$; we have to prove that $\overline{w} t \Vdash_s \overline{C}$. By induction hypothesis on u, $\overline{u}[t/x^{|B|}] \Vdash_s \overline{C}$. By trivial equalities

$$\begin{aligned}
\overline{w}t[s] &= (\lambda x^{|B|} u)[t_1/x_1^{|A_1|} \cdots t_n/x_n^{|A_n|}\ r_1/\alpha_1 \cdots r_k/\alpha_k] t[s] \\
&= (\lambda x^{|B|} u) t[t_1/x_1^{|A_1|} \cdots t_n/x_n^{|A_n|}\ r_1/\alpha_1 \cdots r_k/\alpha_k][s] \\
&= u[t/x^{|B|}][t_1/x_1^{|A_1|} \cdots t_n/x_n^{|A_n|}\ r_1/\alpha_1 \cdots r_k/\alpha_k][s] \\
&= \overline{u}[t/x^{|B|}][s]
\end{aligned}$$

Then by $\overline{u}[s] = \overline{w}t[s]$ and saturation (prop. 1), $\overline{w}t \Vdash_s \overline{C}$.

6. If it is a $\vee I$ rule, say left (the other case is symmetric), then $w = \langle \mathtt{True}, u, d^{|C|}\rangle$, $A = B \vee C$ and $\Gamma \vdash u : B$. So, $\overline{w} = \langle \mathtt{True}, \overline{u}, d^{|C|}\rangle$ and hence $\pi_0 \overline{w}[s] = \mathtt{True}$. We indeed verify that $\overline{u} \Vdash_s \overline{B}$ with the help of induction hypothesis.

7. If it is a $\vee E$ rule, then

$$w = \mathsf{if}\ \mathsf{p}_0 u\ \mathsf{then}\ (\lambda x^{|B|} w_1)(\mathsf{p}_1 u)\ \mathsf{else}\ (\lambda x^{|C|} w_2)(\mathsf{p}_2 u)$$

and $\Gamma \vdash u : B \vee C$, $\Gamma, x : B \vdash w_1 : D$, $\Gamma, y : C \vdash w_2 : D$, $A = D$.
Assume $\mathsf{p}_0 \overline{u}[s] = \mathtt{True}$. By inductive hypothesis $\overline{u} \Vdash_s \overline{B} \vee \overline{C}$. Therefore, $\mathsf{p}_1 \overline{u} \Vdash_s \overline{B}$. Hence

$$\begin{aligned}
\overline{w}[s] &= (\lambda x^{|B|} w_1) \mathsf{p}_1 \overline{u}[t_1/x_1^{|A_1|} \cdots t_n/x_n^{|A_n|}\ r_1/\alpha_1 \cdots r_k/\alpha_k][s] \\
&= w_1[\mathsf{p}_1 \overline{u}/x^{|B|}][t_1/x_1^{|A_1|} \cdots t_n/x_n^{|A_n|}\ r_1/\alpha_1 \cdots r_k/\alpha_k][s] \\
&= w_1[\mathsf{p}_1 \overline{u}/x^{|B|}\ t_1/x_1^{|A_1|} \cdots t_n/x_n^{|A_n|}\ r_1/\alpha_1 \cdots r_k/\alpha_k][s] \\
&= \overline{w_1}[\mathsf{p}_1 \overline{u}/x^{|B|}][s]
\end{aligned}$$

By induction hypothesis, $\overline{w_1}[\mathsf{p}_1 \overline{u}/x^{|B|}] \Vdash_s \overline{D}$. Thus, by $\overline{w_1}[\mathsf{p}_1 \overline{u}/x^{|B|}] = \overline{w}[s]$ and saturation (prop. 1), also $\overline{w} \Vdash_s \overline{D}$.
Symmetrically, if $\mathsf{p}_0 \overline{u}[s] = \mathtt{False}$, we obtain again $\overline{w} \Vdash_s \overline{D}$.

8. If it is the $\forall E$ rule, then $w = ut$, $A = B[t/\alpha^\tau]$ and $\Gamma \vdash u : \forall\alpha^\tau B$. So, $\overline{w} = \overline{u}\overline{t}$. Let $v = \overline{t}[s]$. By inductive hypothesis $\overline{u} \Vdash_s \forall\alpha\overline{B}$ and so $\overline{u}v \Vdash_s \overline{B}[v/\alpha^\tau]$. Since $\overline{u}\overline{t}[s] = \overline{u}v[s]$, by saturation (prop. 1), we conclude that $\overline{u}\overline{t} \Vdash_s \overline{B}[\overline{t}/\alpha^\tau]$.

9. If it is the $\forall I$ rule, then $w = \lambda\alpha^\tau u$, $A = \forall\alpha^\tau B$ and $\Gamma \vdash u : B$ (with α^τ not occurring free in the formulas of Γ). So, $\overline{w} = \lambda\alpha^\tau\overline{u}$, since $\alpha \neq \alpha_1, \ldots, \alpha_k$. Let $t : \tau$ be a closed term of $\mathcal{T}$; by saturation (prop. 1), it is enough to prove that $\overline{w}t = \overline{u}[t/\alpha^\tau] \Vdash_s \overline{B}[t/\alpha^\tau]$, which amounts to show that the induction hypothesis can be applied to u. For this purpose, we observe that, since $\alpha \neq \alpha_1, \ldots, \alpha_k$, for $i = 1, \ldots, n$ we have
$$t_i \Vdash_s \overline{A_i} = \overline{A_i}[t/\alpha^\tau]$$

10. If it is the $\exists E$ rule, then
$$w = (\lambda\alpha^\tau\lambda x^{|B|}t)(\pi_0 u)(\pi_1 u)$$
$\Gamma, x : B \vdash t : A$ and $\Gamma \vdash u : \exists\alpha^\tau.B$. Assume $v = \pi_0\overline{u}[s]$. Then
$$\overline{t}[v/\alpha^\tau, \pi_1\overline{u}/x^{|B|}] \Vdash_s \overline{A}[v/\alpha^\tau] = \overline{A}$$
by inductive hypothesis, whose application being justified by the fact, also by induction, that $\overline{u} \Vdash_s \exists\alpha^{\mathtt{N}}.\overline{B}$ and hence $\pi_1\overline{u} \Vdash_s \overline{B}[v/\alpha^\tau]$. We thus obtain by $\overline{w}[s] = \overline{t}[\pi_0\overline{u}/\alpha^\tau\ \pi_1\overline{u}/x^{|B|}][s]$ and saturation (prop. 1) that
$$\overline{w} \Vdash_s \overline{A}$$

11. If it is the $\exists I$ rule, then $w = \langle t, u\rangle$, $A = \exists\alpha^\tau B$, $\Gamma \vdash u : B[t/\alpha^\tau]$. So, $\overline{w} = \langle\overline{t}, \overline{u}\rangle$; and, indeed, $\pi_1\overline{w} = \overline{u} \Vdash_s \overline{B}[\pi_0\overline{w}/\alpha^\tau] = \overline{B}[\overline{t}/\alpha^\tau]$ since by induction hypothesis $\overline{u} \Vdash_s \overline{B}[\overline{t}/\alpha^\tau]$. By saturation we conclude the thesis.

12. If it is the induction rule, then $w = \lambda\alpha^{\mathtt{N}}\mathsf{R}uv\alpha$, $A = \forall\alpha^{\mathtt{N}}B$, $\Gamma \vdash u : B(0)$ and $\Gamma \vdash v : \forall\alpha^{\mathtt{N}}.B(\alpha) \to B(\mathsf{S}(\alpha))$. So, $\overline{w} = \lambda\alpha^{\mathtt{N}}\mathsf{R}\overline{u}\overline{v}\alpha$. We have to prove that $\overline{w}u \Vdash_s \overline{B}[n/\alpha]$ for all closed normal form of type $\mathtt{N}$. Let $n = u[s]$ be the normal form of $u[s]$: then n is a numeral by the Lemma 5. A plain induction on n shows that
$$\overline{w}n = \mathsf{R}\overline{u}\overline{v}n \Vdash_s \overline{B}[n/\alpha]$$
for $\overline{u} \Vdash_s \overline{B}(0)$ and $\overline{v}i \Vdash_s \overline{B}(i) \to \overline{B}(\mathsf{S}(i))$ for all numerals i by induction hypothesis. If we set $i = n$, the thesis follows by saturation and $\overline{w}u[s] = \overline{w}n[s]$.

13. If it is a Post rule, then $w = u_1 \Cup u_2 \Cup \cdots \Cup u_n$ and $\Gamma \vdash u_i : A_i$. So, $\overline{w} = \overline{u}_1 \Cup \overline{u}_2 \Cup \cdots \Cup \overline{u}_n$. First, suppose that, for $i = 1, \ldots, n$, $\overline{u}_i[s] = \overline{U_i}$ and $\overline{w}[s] = \overline{U}$. By induction hypothesis, $\mathsf{dom}(\overline{U_i}) \cap \mathsf{dom}(s) = \emptyset$, and thus also $\mathsf{dom}(\overline{U}) \cap \mathsf{dom}(s) = \emptyset$. Suppose now that $\overline{U} = \varnothing$; then we have to prove that $\overline{A}[s] = \mathtt{True}$. It suffices to prove that $\overline{A}_1[s] = \overline{A}_2[s] = \cdots = \overline{A}_n[s] = \mathtt{True}$. We have $\overline{U_1} = \cdots = \overline{U_n} = \varnothing$ and by induction hypothesis $\overline{A}_1[s] = \cdots = \overline{A}_n[s] = \mathtt{True}$, since $\overline{u}_i \Vdash_s \overline{A}_i$, for $i = 1, \ldots, n$.

14. If is the excluded middle axiom EM_1, then $w = \mathsf{E}_a$ realizes EM_1 by Prop. 2.

15. If it is a Φ-axiom rule, then

$$w = \lambda x^{\mathtt{N}} \lambda y^{\mathtt{N}} \mathsf{if}\ (\mathsf{P}_a xy \Rightarrow_{\mathtt{Bool}} \mathsf{P}_a x(\Phi_a x))\ \mathsf{then}\ \varnothing\ \mathsf{else}\ (\mathsf{mkupd}\, a\, x\, y)$$

and

$$A = \forall x^{\mathtt{N}} \forall y^{\mathtt{N}}.\ \mathsf{P}_a(x, y) \Rightarrow_{\mathtt{Bool}} \mathsf{P}_a(x, \Phi_a x)$$

Let n, m be two arbitrary numerals. We have to prove that

$$\overline{w} nm \Vdash_s \mathsf{P}_a(n, m) \Rightarrow_{\mathtt{Bool}} \mathsf{P}_a(n, \Phi_a n)$$

There are two cases:

(a) $\mathsf{P}_a(n, m) \Rightarrow_{\mathtt{Bool}} \mathsf{P}_a(n, s_a n) = \mathtt{True}$. In this case, $\overline{w} nm[s] = \varnothing$ and we have only to check that $\mathsf{dom}(s) \cap \mathsf{dom}(\varnothing) = \emptyset$, which is trivial.

(b) $\mathsf{P}_a(n, m) \Rightarrow_{\mathtt{Bool}} \mathsf{P}_a(n, s_a n) = \mathtt{False}$. Then, $\mathsf{P}_a nm = \mathtt{True}$ and $\mathsf{P}_a n s_a(n) = \mathtt{False}$. Moreover

$$\overline{w} nm[s] = \mathsf{mkupd}\, a\, n\, m = \overline{U}$$

with $U = \{(a, n, m)\}$. We have first to check that U is sound (see definition 1): this follows from $\mathsf{P}_a nm = \mathtt{True}$. Then we have to check that $\mathsf{dom}(s) \cap \mathsf{dom}(\overline{U}) = \emptyset$: indeed, $\mathsf{dom}(\overline{U}) = \{(a, n)\}$, and by definition 6, $\mathsf{P}_a n s_a(n) = \mathtt{False}$ implies $(a, n) \notin \mathsf{dom}(s)$. Last, we have to check that $\overline{U} \neq \varnothing$, which is immediate by $U = \{(a, n, m)\}$.

As corollary of the Adequacy theorem 9, we obtain the main theorem.

Theorem 10. *If A is a closed formula such that $\mathsf{HA}^\omega + \mathsf{EM}_1 + \mathsf{SK}_1 \vdash t : A$, then $t \Vdash A$.*

5. Interactive Realizability and Kreisel's No-Counterexample Interpretation of Σ^0_2-formulas: an example of realizer

We now want to relate Interactive Realizability with Kreisel No-Counterexample Interpretation. We construct some terms transforming any witness of Kreisel's Interpretation [20] of any Σ^0_2-formula in an interactive realizer of that formula – and vice versa. Let us fix a Σ^0_2-formula, with $P(x, y)$ predicate of Gödel's system T:

$$\exists x^{\mathtt{N}} \forall y^{\mathtt{N}} P(x, y) \tag{2}$$

We start from the no-counterexample interpretation.

5.1. From the No-Counterexample Interpretation to Interactive Realizability

A witness of the no-counterexample interpretation of (2) is a realizer Ψ – in the sense of Kreisel's modified realizability – of the Herbrand normal form of (2):

$$\forall f^{\mathtt{N} \to \mathtt{N}} \exists x^{\mathtt{N}} P(x, f(x)) \tag{3}$$

That is, $\Psi : (\mathtt{N} \to \mathtt{N}) \to \mathtt{N}$ is a term of $\mathcal{T}$ such that:

$$\forall f^{\mathtt{N}\to\mathtt{N}} P(\Psi f, f(\Psi f)) \tag{4}$$

As it is well known, one has

$$\mathsf{HA}^\omega + \mathsf{EM}_1 + \mathsf{SK}_1 \vdash \forall f^{\mathtt{N}\to\mathtt{N}} P(\Psi f, f(\Psi f)) \to \exists x^{\mathtt{N}} \forall y^{\mathtt{N}} P(x, y)$$

The proof is classical and goes as follows. Suppose (4) and assume without loss of generality that

$$\mathsf{P}_0(x, y) \equiv \neg_{\mathtt{Bool}} P(x, y)$$

We recall that Φ_0 is the Skolem map for $\exists y^{\mathtt{N}}\, \mathsf{P}_0(x, y)$. Let $x = \Psi\Phi_0$. Then, by (4) with $f = \Phi_0$, we deduce $P(\Psi\Phi_0, \Phi_0(\Psi\Phi_0))$, that is

$$P(x, \Phi_0(x))$$

and equivalently

$$\neg_{\mathtt{Bool}} \mathsf{P}_0(x, \Phi_0(x))$$

By SK_1 we obtain the Skolem axiom for Φ, therefore from $\neg_{\mathtt{Bool}} \mathsf{P}_0(x, \Phi_0(x))$ we get

$$\forall y^{\mathtt{N}} \neg \mathsf{P}_0(x, y)$$

which is equivalent to $\forall y^{\mathtt{N}} P(x, y)$. Thus we conclude (2).

By the Adequacy theorem 9, we know that an interactive realizer Ω of

$$\forall f^{\mathtt{N}\to\mathtt{N}} \exists x^{\mathtt{N}} P(x, f(x)) \to \exists x^{\mathtt{N}} \forall y^{\mathtt{N}} P(x, y)$$

indeed does exist. Since

$$\lambda f^{\mathtt{N}\to\mathtt{N}} \langle \Psi f, \varnothing \rangle) \Vdash \forall f^{\mathtt{N}\to\mathtt{N}} \exists x^{\mathtt{N}} P(x, f(x))$$

we have that $\Omega(\lambda f^{\mathtt{N}\to\mathtt{N}} \langle \Psi f, \varnothing \rangle)$ is a interactive realizer of (2).

It is instructive however to build directly Ω, as example, by using the aforementioned classical proof as a source of inspiration. The witness to (2) coming from the proof is just $\Psi(\Phi_0)$. This latter term is not computable, but we suppose to have an approximation $s : \mathtt{N}^2 \to \mathtt{N}$ of Φ. When we compute

$$\Psi(\Phi_0)[s] = \Psi(s_0) = n$$

if we are lucky we obtain a numeral n which is a witness to (2). But in general this is not the case, and we must be prepared to test the result of our computation and to correct s if n is a wrong witness. Indeed, the term

$$\lambda y^{\mathtt{N}}\, \mathsf{if}\;\; Pny \;\mathsf{then}\; \varnothing \;\mathsf{else}\; \mathsf{mkupd}\, 0\, n\, y$$

does the job, as the next proposition says.

Proposition 3 (From the N.C.I. to Learning-Based Realizability). *Suppose* $\Psi : (\mathtt{N} \to \mathtt{N}) \to \mathtt{N}$ *is a term of* $\mathcal{T}$ *such that:*

$$\forall f^{\mathtt{N}\to\mathtt{N}} P(\Psi f, f(\Psi f))$$

Then

$$\langle \Psi(\Phi_0), \lambda y^{\mathtt{N}}\, \mathsf{if}\;\; P\Psi(\Phi_0)y \;\mathsf{then}\; \varnothing \;\mathsf{else}\; \mathsf{mkupd}\, 0\, \Psi(\Phi_0)\, y \rangle \Vdash \exists x^{\mathtt{N}} \forall y^{\mathtt{N}} P(x, y)$$

Proof. Let $s : \mathtt{N}^2 \to \mathtt{N}$ be a closed term of $\mathcal{T}$, $s_0 = \Phi_0[s]$ be the corresponding approximation of the Skolem map Φ_0 for $\exists y^{\mathtt{N}} \mathsf{P}_0(x, y)$, and n be the normal form of $\Psi(s_0)$. Then n is a numeral by Lemma 5. By definition of interactive realizability, we have to show that, if we compute

$$\Psi(\Phi_0)[s] = \Psi(s_0) = n$$

then we have

$$\lambda y^{\mathtt{N}}\, \mathsf{if}\ P\Psi(\Phi_0)y\ \mathsf{then}\ \varnothing\ \mathsf{else}\ \mathsf{mkupd}\,0\,\Psi(\Phi_0)\,y \Vdash_s \forall y^{\mathtt{N}} P(n, y)$$

Thus we must show that, fixed any numeral m,

$$\mathsf{if}\ P\Psi(\Phi_0)m\ \mathsf{then}\ \varnothing\ \mathsf{else}\ \mathsf{mkupd}\,0\,\Psi(\Phi_0)\,m\rangle \Vdash_s P(n, m)$$

Compute

$$\mathsf{if}\ P\Psi(\Phi_0)m\ \mathsf{then}\ \varnothing\ \mathsf{else}\ \mathsf{mkupd}\,0\,\Psi(\Phi_0)\,m[s] = \mathsf{if}\ Pnm\ \mathsf{then}\ \varnothing\ \mathsf{else}\ \mathsf{mkupd}\,0\,n\,m = \overline{U}$$

for some $U \in \mathbb{U}$. There are two cases for U:

1. $U = \varnothing$. Then $Pnm = \mathtt{True}$ and thus we obtain the thesis:

$$\mathsf{if}\ P\Psi(\Phi_0)m\ \mathsf{then}\ \varnothing\ \mathsf{else}\ \mathsf{mkupd}\,0\,\Psi(\Phi_0)\,m \Vdash_s P(n, m)$$

   by definition of realizability for atomic formulas.

2. $U = \{(0, n, m)\}$. Then $Pnm = \mathtt{False}$, and hence $\mathsf{P}_0nm = \mathtt{True}$ by $\mathsf{P}_0(x, y) \equiv \neg_{\mathtt{Bool}} P(x, y)$. Since

$$\forall f^{\mathtt{N}\to\mathtt{N}} P(\Psi f, f(\Psi f))$$

   by letting $f = s_0$ and substituting Ψs_0 with n, we obtain $Pns_0(n) = \mathtt{True}$; therefore $\mathsf{P}_0n\Phi_0[s](n) = \mathsf{P}_0ns_0(n) = \mathtt{False}$. Therefore U is sound and $\mathsf{dom}(U) \cap \mathsf{dom}(s) = \emptyset$. That is, we have the thesis:

$$\mathsf{if}\ P\Psi(\Phi_0)m\ \mathsf{then}\ \varnothing\ \mathsf{else}\ \mathsf{mkupd}\,0\,\Psi(\Phi_0)\,m \Vdash_s P(n, m)$$

5.2. From Interactive Realizability to the No-Counterexample Interpretation

It is trivial to show that

$$\mathsf{HA}^\omega + \mathsf{EM}_1 + \mathsf{SK}_1 \vdash \exists x^{\mathtt{N}} \forall y^{\mathtt{N}} P(x, y) \to \forall f^{\mathtt{N}\to\mathtt{N}} \exists x^{\mathtt{N}} P(x, f(x))$$

since any x such that $\forall y^{\mathtt{N}} P(x, y)$ is such that $P(x, f(x))$, whatever f is. Hence, given any interactive learning-based realizer

$$t \Vdash \exists x^{\mathtt{N}} \forall y^{\mathtt{N}} P(x, y)$$

and by following the idea of the trivial proof above, we obtain that

$$\lambda f^{\mathtt{N}\to\mathtt{N}} \langle \pi_0 t, (\pi_1 t) f(\pi_0 t)\rangle \Vdash \forall f^{\mathtt{N}\to\mathtt{N}} \exists x^{\mathtt{N}} P(x, f(x))$$

By theorem 8, we obtain a term with the properties of Ψ. According to the proof of theorem 8, that term takes an $f : \mathtt{N} \to \mathtt{N}$ and computes the sequence

$$s_0 := \lambda x^{\mathtt{N}}\, 0$$
$$s_{n+1} := s_n \oplus (\pi_1 t) f(\pi_0 t)[s_n]$$

until an m such that $(\pi_1 t) f(\pi_0 t)[s_m] = \varnothing$ is found; then it returns $\pi_0 t[s_m]$. It is more efficient, however, to start with

$$s_0 := f$$

since by theorem 7 the produced sequence converges as well to a zero.

6. Interactive Realizability as Friedman's Translation + Kreisel's Modified Realizability

In this subsection we show that the notion of Interactive Realizability for $\mathsf{HA}^\omega + \mathsf{EM}_1 + \mathsf{SK}_1$ represents a new way of using Friedman's translation. More precisely, Interactive Realizability is exactly the same as the notion of Kreisel's modified realizability for HA^ω applied to our restricted Friedman translation of formulas. More precisely, we claim that the notion $t \Vdash B$ is equivalent to the notion $\forall s^{\mathtt{N}^2 \to \mathtt{N}} \in \mathcal{T}.\ t[s]\ \mathsf{mr}\ B[s]^{\mathscr{A}(s)}$.

Before we begin our argument, we recall the definition of modified realizability mr (Kreisel [20]). We denote with $\mathcal{L}$ the set of terms and formulas obtained from the terms and formulas of $\mathcal{L}_{\text{Class}}$ by replacing the constant Φ with some term $s : \mathtt{N}^2 \to \mathtt{N}$ of $\mathcal{T}$.

Definition 11 (Modified Realizability). *Assume $s : \mathtt{N}^2 \to \mathtt{N}$ is a closed term of $\mathcal{T}$, t is a closed term of $\mathcal{T}$, $D \in \mathcal{L}$ is a closed formula, and $t : |D|$. We define by induction on D the relation $t\ \mathsf{mr}\ D$:*

1. $t\ \mathsf{mr}\ Q$ *if and only if* $Q = \mathtt{True}$
2. $t\ \mathsf{mr}\ A \wedge B$ *if and only if* $\pi_0 t\ \mathsf{mr}\ A$ *and* $\pi_1 t\ \mathsf{mr}\ B$
3. $t\ \mathsf{mr}\ A \vee B$ *if and only if either* $\mathsf{p}_0 t = \mathtt{True}$ *and* $\mathsf{p}_1 t\ \mathsf{mr}\ A$*, or* $\pi_0 t = \mathtt{False}$ *and* $\mathsf{p}_1 t\ \mathsf{mr}\ B$
4. $t\ \mathsf{mr}\ A \to B$ *if and only if for all u, if $u\ \mathsf{mr}\ A$, then $tu\ \mathsf{mr}\ B$*
5. $t\ \mathsf{mr}\ \forall x^\tau A$ *if and only if for all closed terms $u : \tau$ of $\mathcal{T}$, $tu\ \mathsf{mr}\ A[u/x]$*
6. $t\ \mathsf{mr}\ \exists x^\tau A$ *if and only for some closed term $u : \tau$ of $\mathcal{T}$, $\pi_0 t = u$ and $\pi_1 t\ \mathsf{mr}\ A[u/x]$*

It is technically more convenient to define directly a realizability relation mrf_s such that $t\, \mathsf{mrf}_s\, B[s]$ is equivalent (modulo some inessential adjustments in the atomic case) to the relation $t\, \mathsf{mr}\, B[s]^{\mathscr{A}(s)}$. When Q is atomic, the relation $t\ \mathsf{mr}\ Q[s]^{\mathscr{A}(s)}$ is defined as

$$t\ \mathsf{mr}\ Q[s] \vee \exists x^{\mathtt{N}} \exists y^{\mathtt{N}} \exists z^{\mathtt{N}}.\ \mathscr{T}xyz \wedge \neg \mathscr{T}xys(x,y)$$

So, either $Q[s] = \mathtt{True}$ or $\mathsf{p}_2 t$ contains a triple of numerals n, m, l such that $\mathscr{T}nml \wedge \neg \mathscr{T}nms(n,m)$ is true. Thus it is better to define directly t as term of type $\mathtt{U}$ which reduces to an update, non-empty and containing such numerals n, m, l whenever Q is false.

Definition 12 (mr **Combined with the** $\mathscr{A}(s)$**-Translation).** *Assume $s : \mathtt{N}^2 \to \mathtt{N}$ is a closed term of $\mathcal{T}$, t is a closed term of $\mathcal{T}$, $D \in \mathcal{L}$ is a closed formula of $\mathcal{L}$, and $t : |D|$. We define by induction on D the relation $t \ \mathsf{mrf}_s \ D$:*

1. *$t \ \mathsf{mrf}_s \ Q$ if and only if*
   - *$t = \overline{U}$ implies that for all $(n, m, l) \in U$, $\mathscr{T}nml = \mathtt{True}$ and $\mathscr{T}nms(n, m) = \mathtt{False}$*
   - *$t = \varnothing$ implies $Q = \mathtt{True}$*

2. *$t \ \mathsf{mrf}_s \ A \wedge B$ if and only if $\pi_0 t \ \mathsf{mrf}_s \ A$ and $\pi_1 t \ \mathsf{mrf}_s \ B$*

3. *$t \ \mathsf{mr} \ A \vee B$ if and only if either $\mathsf{p}_0 t = \mathtt{True}$ and $\mathsf{p}_1 t \ \mathsf{mr} \ A$, or $\pi_0 t = \mathtt{False}$ and $\mathsf{p}_1 t \ \mathsf{mr} \ B$*

4. *$t \ \mathsf{mrf}_s \ A \to B$ if and only if for all u, if $u \ \mathsf{mrf}_s \ A$, then $tu \ \mathsf{mrf}_s \ B$*

5. *$t \ \mathsf{mrf} \ \forall x^\tau A$ if and only if for all closed terms $u : \tau$ of $\mathcal{T}$, $tu \ \mathsf{mrf} \ A[u/x]$*

6. *$t \ \mathsf{mrf} \ \exists x^\tau A$ if and only for some closed term $u : \tau$ of $\mathcal{T}$, $\pi_0 t = u$ and $\pi_1 t \ \mathsf{mrf} \ A[u/x]$*

We are now able to characterize learning-based realizability $\Vdash$ as a Friedman translation combined with Kreisel's modified realizability.

Theorem 11 (Characterization of Interactive Realizability). *Let $t \in \mathcal{T}_{\mathit{Class}}$ and $s : \mathtt{N}^2 \to \mathtt{N} \in \mathcal{T}$. Then, for every $B \in \mathcal{L}_{\mathit{Class}}$*

$$t \Vdash_s B \iff t[s] \, \mathsf{mrf}_s \, B[s]$$

Proof. The thesis is proved by routine induction on B.

1. $B = Q$, with Q atomic. Then $t[s] \ \mathsf{mrf}_s \ Q[s]$, by definition 12, holds if and only if:
   - $t[s] = \overline{U}$ implies that for all $(n, m, l) \in U$, $\mathscr{T}nml = \mathtt{True}$ and $\mathscr{T}nms(n, m) = \mathtt{False}$
   - $t[s] = \varnothing$ implies $Q[s] = \mathtt{True}$

   Indeed, this is exactly the definition 10 of $t \Vdash_s Q$, provided one makes some additional hypothesis on the enumeration $\mathsf{P}_0, \mathsf{P}_1, \ldots$ of definition 1. For example, it is enough to assume that for each numeral n, $\mathsf{P}_n = \mathscr{T}n$.

2. $B = C \wedge D$. Then $t \Vdash_s C \wedge D$ if and only if $\pi_0 t \Vdash_s C$ and $\pi_1 t \Vdash_s D$ if and only if (by induction hypothesis) $\pi_0 t[s] \ \mathsf{mrf}_s \ C[s]$ and $\pi_1 t[s] \ \mathsf{mrf}_s \ D[s]$ if and only if $t[s] \ \mathsf{mrf}_s (C \wedge D)[s]$.

3. $B = C \vee D$. Assume $\mathsf{p}_0 t[s] = \mathtt{True}$ (the case $\mathsf{p}_0 t[s] = \mathtt{False}$ is symmetrical). Then, $t \Vdash_s C \vee D$ if and only if $\mathsf{p}_1 t \Vdash_s C$ if and only if (by induction hypothesis) $\mathsf{p}_1 t[s] \ \mathsf{mrf}_s \ C[s]$ if and only if $t[s] \ \mathsf{mrf} \ (C \vee D)[s]$ by the very definition 12 of mrf_s.

4. $B = C \to D$. Assume $t \Vdash_s C \to D$. We want to prove that $t[s] \Vdash_s (C \to D)[s]$. Thus, we have to suppose $u \ \mathsf{mrf}_s \ C[s]$ and conclude that $t[s]u \ \mathsf{mrf}_s \ D[s]$. Since $u = u[s]$ (u is a closed term of $\mathcal{T}$ by definition 12), by induction hypothesis we obtain that $u \ \mathsf{mrf}_s \ C$ and hence that $tu \Vdash_s D$. By induction hypothesis, $t[s]u = tu[s] \ \mathsf{mrf}_s \ D[s]$, which is what we wanted to show.
Conversely, assume $t \ \mathsf{mrf}_s \ (C \to D)[s]$. We want to prove that $t \Vdash_s C \to D$. Thus, we have to suppose $u \ \mathsf{mrf}_s \ C$ and conclude that $tu \ \mathsf{mrf}_s \ D$. By induction hypothesis, we obtain that $u[s] \ \mathsf{mrf}_s \ C[s]$ and hence that $tu[s] \Vdash_s D[s]$. By induction hypothesis again, $tu \ \mathsf{mrf}_s \ D$, which is what we wanted to show.

5. $B = \forall x^\tau C$. Assume $t \Vdash_s \forall x^\tau C$ and let $u : \tau$ an arbitrary closed term of $\mathcal{T}$. Then $tu \Vdash_s C[u/x]$ and by induction hypothesis $t[s]u = tu[s] \ \mathsf{mrf}_s \ C[u/x][s] = C[s][u/x]$. We have thus proved that $t[s] \ \mathsf{mrf}_s \ \forall x^\tau C[s]$. Similarly, one proves that $t[s] \ \mathsf{mrf}_s \ \forall x^\tau C[s]$ implies $t \Vdash_s \forall x^\tau C$.

6. $B = \exists x^\tau C$. Assume $\mathsf{p}_0 t[s] = u$. Then $t \Vdash_s \exists x^\tau C$ if and only if $\mathsf{p}_1 t \Vdash_s C[u/x]$ if and only (by induction hypothesis) $\mathsf{p}_1 t[s] \ \mathsf{mrf}_s \ C[u/x][s] = C[s][u/x]$ if and only if $t[s] \ \mathsf{mrf}_s \ \exists x^\tau C[s]$.

Finally, we are able to prove the correctness property of restricted Friedman's translation which we claimed in §2.

Theorem 12 (Correctness of the Restricted Friedman Translation). *Given any atomic predicate $P(x, y)$, the following holds:*

$$\mathsf{HA}^\omega \vdash (\forall x^{\mathtt{N}} \exists y^{\mathtt{N}} P(x, y))^{\mathscr{A}(s)} \implies \mathsf{HA}^\omega \vdash \forall x^{\mathtt{N}} \exists y^{\mathtt{N}} P(x, y)$$

Proof. Let us consider an arbitrary Π^0_2-formula $\forall x^{\mathtt{N}} \exists y^{\mathtt{N}} P(x, y)$. By applying Kreisel's modified realizability to any proof in HA^ω of $(\forall x^{\mathtt{N}} \exists y^{\mathtt{N}} P(x, y))^{\mathscr{A}(s)}$, one obtains a term $t[s]$ of Gödel's system T such that

$$\forall s^{\mathtt{N} \to \mathtt{N}}.\ t[s] \ \mathsf{mr} \ (\forall x^{\mathtt{N}} \exists y^{\mathtt{N}} P(x, y))^{\mathscr{A}(s)}$$

and thus

$$\forall s^{\mathtt{N} \to \mathtt{N}}.\ t[s] \ \mathsf{mrf}_s \ \forall x^{\mathtt{N}} \exists y^{\mathtt{N}} P(x, y)$$

by definition of mrf. By theorem 11, for some t' we have

$$t' \Vdash \forall x^{\mathtt{N}} \exists y^{\mathtt{N}} P(x, y)$$

Moreover, by theorem 8, from t' one can extract a term $u : \mathtt{N} \to \mathtt{N}$ of Gödel's system T such that for every numeral n, $P(n, u(n)) = \mathtt{True}$. The proof is carried out in HA^ω, hence one obtains that

$$t' \Vdash \forall x^{\mathtt{N}} \exists y^{\mathtt{N}} P(x, y) \implies \mathsf{HA}^\omega \vdash \forall x^{\mathtt{N}} \exists y^{\mathtt{N}} P(x, y)$$

Therefore,

$$\mathsf{HA}^\omega \vdash (\forall x^{\mathtt{N}} \exists y^{\mathtt{N}} P(x, y))^{\mathscr{A}(s)} \implies \mathsf{HA}^\omega \vdash \forall x^{\mathtt{N}} \exists y^{\mathtt{N}} P(x, y)$$

which is the thesis.

[1] F. Aschieri, S. Berardi, *Interactive Learning-Based Realizability for Heyting Arithmetic with* EM_1, Logical Methods in Computer Science, 2010.
[2] F. Aschieri, *Interactive Learning Based Realizability and 1-Backtracking Games*, Proceedings of Classical Logic and Computation 2010, Electronic Proceedings in Theoretical Computer Science, 2011.
[3] F. Aschieri, *Learning, Realizability and Games in Classical Arithmetic*, PhD Thesis, 2011. http://arxiv.org/abs/1012.4992
[4] F. Aschieri, *Transfinite Update Procedures for Predicative Systems of Analysis*, Proceedings of Computer Science Logic, 2011.
[5] F. Aschieri, *A Constructive Analysis of Learning in Peano Arithmetic*, Annals of Pure and Applied Logic, 2011, doi:10.1016/j.apal.2011.12.04
[6] J. Avigad, *Update Procedures and 1-Consistency of Arithmetic*, Mathematical Logic Quarterly, volume 48, 2002.
[7] J. Avigad, *A realizability Interpretation for Classical Arithmetic*, in Buss, Hjek, and Pudlk eds., Logic Colloquium '98, Lecture Notes in Logic 13, AK Peters, 57-90, 2000.
[8] S. Berardi, *Classical Logic as Limit Completion*, MSCS, Vol. 15, n.1, 2005, pp.167-200.
[9] S. Berardi and U. de' Liguoro, *Interactive Realizers. A New Approach to Program Extraction from non-Constructive Proofs*, TOCL, 2010.
[10] U. Berger, H. Schwichtenberg, *Program Extraction from Classical Proofs*, Logic and Computational Complexity Workshop 1994, Lecture Notes in Computer Science, vol. 960, Springer, 1995.
[11] T. Coquand, *A Semantic of Evidence for Classical Arithmetic*, Journal of Symbolic Logic 60, pag 325-337,1995.
G
[12] H. Friedman, *Classically and Intuitionistically Provable Recursive Functions*, Lecture Notes in Mathematics, 1978, Volume 669/1978, 21-27.
[13] K. Gödel *Uber eine bisher noch nicht ben utzte Erweiterung des niten Standpunktes*, Dialectica 12, 280287 (reproduced with English translation, in [Gödel 1990], 240251.
[14] G. Gentzen, *Die Widerspruchsfreiheit der reinen Zahlentheorie*. Mathematische Annalen, 112:493-565, 1935. English translation: The consistency of elementary number theory, in Szabo [465], pages 132-200.
[15] G. Gentzen, *Untersuchungen fiber das logische Schliessen. Mathematische Zeitschrift, 39:176-210, 405-431, 1935. English translation: Investigations into logical deduction, in Szabo [465], pages 68-131*
[16] J.-Y. Girard, *Proofs and Types*, Cambridge University Press (1989).
[17] E. M. Gold, *Limiting Recursion*, Journal of Symbolic Logic 30, pag. 28-48 (1965).
[18] S. C. Kleene, *On the Interpretation of Intuitionistic Number Theory*, Journal of Symbolic Logic 10(4), pag 109-124 (1945).
[19] U. Kohlenbach, *Applied Proof Theory*, Springer-Verlag, Berlin, Heidelberg, 2008.
[20] G. Kreisel, *On the Interpretation of non-Finitist Proofs, Part II: Interpretation of Number Theory, Applications*, Journal of Symbolic Logic, vol. 17, 1952.
[21] G. Kreisel, *On Weak Completeness of Intuitionistic Predicate Logic*, Journal of Symbolic Logic, vol. 27, 1962.
[22] J-L. Krivine, *Typed lambda-calculus in classical Zermelo-Fraenkel set theory*, Archive for Mathematical Logic, 40(3):189205, 2001.
[23] G. Mints, S. Tupailo, W. Bucholz, *Epsilon Substitution Method for Elementary Analysis*, Archive for Mathematical Logic, volume 35, 1996
[24] G. Mints, S. Tupailo, *Epsilon Substitution Method for the Ramified Language and* Δ^1_1*-Comprehension Rule*, Logic and Foundations of Mathematics, 1999.
[25] A. Miquel, *Relating classical realizability and negative translation for existential witness extraction.* In Typed Lambda Calculi and Applications (TLCA 2009), pp. 188-202, 2009.
[26] P. Odifreddi, *Classical Recursion Theory*, Studies in Logic and Foundations of Mathematics, Elsevier, 1989
[27] P. Oliva, T. Streicher, *On Krivine Realizability Interpretation of Second-Order Classical Arithmetic*, Fundamenta Informaticae, 2008.
[28] H. Schwichtenberg, A. Troelstra, *Basic Proof Theory*, Cambridge University Press, 1996
[29] M. H. Sorensen, P. Urzyczyn, *Lectures on the Curry-Howard isomorphism*, Studies in Logic and the Foundations of Mathematics, vol. 149, Elsevier, 2006.
[30] C. Spector, *Provably Recursive Functionals of Analysis: a Consistency Proof of Analysis by an Extension of Principles in Current Intuitionistic Mathematics*, Dekker (ed.), Recursive Function

Theory: Proceedings of Symposia in Pure Mathematics, vol. 5. AMS, Providence, 1962
[31] A. Troelstra, D. van Dalen, *Constructivism in Mathematics, vol. I*, North-Holland, 1988.
[32] H. Towsner, *A Realizability Interpretation of Classical Analysis*, Archive for Mathematical Logic, vol. 43, 2005.
[33] A. Troelstra, *Metamathematical Investigations of Intuitionistic Arithmetic and Analysis*, Lecture Notes in Mathematics, Springer-Verlag, Berlin-Heidelber-NewYork, 1973.